
**IMPORTANT NOTE CONCERNING THE FOLLOWING
PAGES**

**THE PAGES WHICH FOLLOW HAVE BEEN FILMED
TWICE IN ORDER TO OBTAIN THE BEST
REPRODUCTIVE QUALITY**

**USERS SHOULD CONSULT ALL THE PAGES
REPRODUCED ON THE FICHE IN ORDER TO OBTAIN
A COMPLETE READING OF THE TEXT.**

**REMARQUE IMPORTANTE CONCERNANT LES
PAGES QUI SUIVENT**

**LES PAGES SUIVANTES ONT ÉTÉ REPRODUITES EN
DOUBLE AFIN D'AMÉLIORER LA QUALITÉ DE
REPRODUCTION**

**LES UTILISATEURS DOIVENT CONSULTER TOUTES
LES PAGES REPRODUITES SUR LA FICHE AFIN
D'OBTENIR LA LECTURE DU TEXTE INTÉGRAL**

Micromedia
ProQuest

20 Victoria Street
Toronto, Ontario M5C 2N8
Tel.: (416) 362-5211
Toll Free: 1-800-387-2689
Fax: (416) 362-6161
Email: info@micromedia.on.ca



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Defence R&D Canada Second Multi-Level Security Meeting, April 2005

J. Savoie

Defence R&D Canada – Ottawa

TECHNICAL MEMORANDUM

DRDC Ottawa TM 2005-249

December 2005

Canada



Defence R&D Canada Second Multi-Level Security Meeting, April 2005

J. Savoie

Defence R&D Canada – Ottawa

Technical Memorandum

DRDC Ottawa TM 2005-249

December 2005

- © Her Majesty the Queen as represented by the Minister of National Defence, 2005
- © Sa majesté la reine, représentée par le ministre de la Défense nationale, 2005

Abstract

The Second Multi-Level Security (MLS) meeting in a series was held on April 6, 2005 at Defence R&D Canada (DRDC) Ottawa. The purpose of these meetings is to bring together researchers, developers, and practitioners in multi-level security (MLS), from both military and civilians sectors, and to provide a forum for dialog and interchange. The second meeting theme was short-to-medium term solutions for current MLS issues for the Department of National Defence or organizations within the Canadian government. The second meeting's invited presentations, discussions and questions to participants are provided and analysed. Moreover, a conclusion and a motivated recommendation are given. It is recommended that a multi-security domain working group be established.

Résumé

Le second meeting d'une série sur la sécurité des systèmes d'information multi niveaux (MLS) a eu lieu le 6 avril 2005 à Recherches et développement pour la défense Canada (DRDC) Ottawa. Le but de ces meetings est de réunir des chercheurs, des développeurs, et des utilisateurs de systèmes MLS venant de milieux militaires et civils dans le but d'échanger et de partager de l'information. Ce second meeting avait comme thème les solutions à court ou moyen terme de problèmes MLS courants du ministère la défense nationale ou d'organismes du gouvernement canadien. Les résultats des présentations des invités, des discussions entre participants, et des questions posés à ceux-ci sont colligés et analysés. De plus, une conclusion et une recommandation motivée sont données. Il est recommandé qu'un groupe de travail sur les multi domaines de sécurité soit formé.

This page intentionally left blank

Executive summary

The Second DRDC Meeting on Multi-Level Security (MLS) was held at DRDC Ottawa on April 6, 2005. The meeting theme was short-to-medium term solutions for current MLS problems within Department of National Defence (DND) or Canadian government organizations. Participants included people from the Network Information Operations (NIO) section of DRDC Ottawa, DND, the Collaborative Capability Definition Engineering and Management Demonstrator (CapDEM), the Canadian Forces (CF), Other Government Departments (OGDs), and DND contractors.

Four presentations were given. The first three presentations involved discussions on the issue of the control of information flows across security domain boundaries, which is a fundamental MLS issue. The first presentation was on a Project Arrangement commissioned by The Technical Cooperation Program (TTCP) C3I to demonstrate network management across security domain boundaries in a coalition network consisting of three national coalition sub-networks (Canada, US, and Australia) connected to their respective national networks. The second presentation was on The Segregation and Hardening of Systems via Virtual Machines (VMs) to provide information sharing mechanisms across security domains in workstations. The third presentation gave an overview of MLS security domain architecture based on the assignment of a network to each security domain. The architecture was described through the concept of linked System-High Enclaves (SHEs). An architecture based on a single network was also presented. The last presentation was on the application of a facial recognition system developed at DRDC Ottawa to provide assurance that, at any time, a user logged onto a workstation is the same one that logged on originally. This is a low-cost solution that improves workstation security.

During the discussion session, participants were asked to provide their input on short-to-medium MLS solutions for a case study. Points covered included the domain architecture to be selected, characteristics of this architecture, and information flow control systems.

The following six questions were asked of participants at the Wrap Up and final session: What is the single most important problem to be addressed by an MLS solution in immediate terms? What is the most promising technology to begin implementing a solution in the short term? What would be the most promising MLS research areas of value for DND? What are the most important issues to be addressed at the next meeting? What are the characteristics of the Certification and Accreditation (C&A) process? and What would be the characteristics of a better C&A process and how this can be implemented?

From the information gathered through presentations, discussions, and answers to the questions, it is recommended that a multi security domain working group be created among stakeholders to synergize development of multi security domain solutions; to facilitate the implementation of such solutions within DND and the CF; and, to improve the certification process for those solutions.

Savoie, J. 2005. Defence R&D Canada Second Multi-Level Security Meeting. DRDC Ottawa TM 2005-249, Defence R&D Canada – Ottawa.

Sommaire

La deuxième réunion du RDDC Ottawa sur la sécurité à multi-niveaux (MLS) a eu lieu au RDDC Ottawa le 6 avril 2005. Le thème de réunion était sur les solutions à court ou moyen terme de problèmes MLS courants du ministère la défense nationale (MDN) ou d'organismes du gouvernement canadien. Les participants à la réunion incluaient des gens de la Section d'opérations de réseau du RDDC Ottawa, du MDN, de CapDEM, des forces canadiennes (FC), d'autres services gouvernementaux, et d'entrepreneurs du MDN.

Quatre présentations ont été données. Les trois premières ont donné lieu à des discussions sur le problème du contrôle des flots d'information entre domaines de sécurité : ce problème est fondamental dans tout système MLS. La première présentation était sur un projet du TTCP C3I sur la réalisation d'un réseau de coalition fait de trois sous réseaux nationaux (Canada, USA, et Australie) reliés chacun à leur réseau national. La deuxième présentation était sur les machines virtuelles (VMs) qui sont des systèmes qui peuvent fournir des mécanismes de transfert d'information entre domaines de sécurité pour des postes de travail. La troisième présentation a porté sur l'architecture usuelle des domaines de sécurité. Celle-ci attribue à chaque domaine de sécurité un réseau. L'architecture utilise le concept d'enclave fonctionnant en mode haut (SHEs). Une architecture basée sur un réseau unique a été également présentée. La dernière présentation était sur un système d'identification facial développé au RDDC Ottawa fournissant l'assurance qu'à tout moment d'une session, l'utilisateur d'un poste de travail est celui qui a été authentifié à l'origine. C'est une solution peu coûteuse qui améliore la sécurité des postes de travail.

Durant la session de discussion, les participants ont été invités à fournir leurs idées sur des solutions MLS de court ou moyen terme pour une étude de cas. Les points couverts ont porté sur l'architecture de domaine à choisir, les caractéristiques de cette architecture, et des systèmes de contrôle de flots entre domaines de sécurité.

À la session finale, les participants ont répondu aux six questions suivantes: Quel est le problème MLS le plus important qui peut être résolu en terme immédiat ? Quelle est la technologie la plus prometteuse permettant des solutions MLS à court terme ? Quels sont les secteurs les plus prometteurs de recherche en MLS pour le MDN ? Quelles sont les questions les plus importantes à considérer lors de la prochaine réunion ? Quelles sont les caractéristiques du processus de certification et d'accréditation (C&A) actuel? et quelles seraient les caractéristiques d'un meilleur processus de C&A et comment celui-ci pourrait-il être mis en place?

A partir de l'information recueillie des présentations, des discussions, et des réponses aux questions, il est recommandé qu'un groupe de travail sur les multi domaines de sécurité soit créé pour mettre en synergie les acteurs intéressés au développement de solutions multi domaines de sécurité; pour faciliter la réalisation de telles solutions pour le MDN ou les FCs; et pour améliorer les processus de certification de ces solutions.

Savoie, J. 2005. La deuxième réunion du RDDC Ottawa sur la sécurité à multi-niveaux. RDDC Ottawa TM 2005-249, R & D pour la défense Canada – Ottawa.

Table of contents

Abstract.....	i
Executive summary	iii
Sommaire	iv
Table of contents.....	v
List of figures.....	viii
List of tables	ix
1. Introduction	1
2. Objectives/Expectations of stakeholders	3
3. Presentations	4
3.1 Presentation 1: MLM: Coordinating Network Management across Security Boundaries using Policy Resolution.....	4
3.1.1 Abstract.....	4
3.1.2 Questions from stakeholders and responses	4
3.2 Presentation 2: Segregation & Hardening of Systems via Virtual Machines ...	6
3.2.1 Abstract.....	6
3.2.2 Questions from stakeholders and responses	6
3.3 Presentation 3: Overview of some MLS architectures and MLS solutions	9
3.3.1 Abstract.....	9
3.3.2 Questions from stakeholders and responses	9
3.3.3 Comments from stakeholders	10
3.4 Presentation 4: A trusted user monitoring system with biometrics	10
3.4.1 Abstract.....	10
3.4.2 Questions from stakeholders and responses	11
4. Discussion session	13
4.1 Characteristics of the current IA architecture	13
4.1.1 Enclave characteristics	13
4.1.2 Information Management characteristics	13
4.1.3 Why classification of networks is useful.....	14

4.2	A case study: CapDEM	14
4.2.1	CapDEM's mission.....	14
4.2.2	CapDEM's MLS objectives.....	15
4.2.3	CapDEM's assumptions	15
4.2.4	Solution 1: Linked System-High Enclaves (SHEs)	15
4.2.5	A single network solution.....	17
5.	Wrap up session.....	18
5.1	What is the single most important problem to be addressed by an MLS solution in immediate term? What is the most promising technology to begin implementing a solution in the short term?	18
5.1.1	Certification and Accreditation.....	18
5.1.2	Multi security domain solutions	18
5.1.3	Labelling.....	18
5.1.4	Definition of business processes.....	19
5.2	What would be the most promising MLS research areas in term of value for DND?	19
5.3	What are the most important issues to be addressed at the next meeting?	19
5.4	What are the characteristics of the Certification& Accreditation process? What would be the characteristics of a better C&A process? How can this be implemented?20	
5.4.1	Roles of security policies in system evaluation.....	20
5.4.2	Security policy context	20
5.4.3	Rationales of security policy contexts	21
5.4.4	System evaluation versus risk evaluation	21
5.4.5	Other elements of system evaluations	21
5.4.6	Risk evaluation methodology	21
6.	Conclusions	22
7.	Recommendations	23
	References.....	25
	List of acronyms	26
	Appendix A: Generic CBIS architecture defined and compared	29
A.1	Definition of information domain.....	29
A.2	Traditional architecture for a single information domain	29
A.3	A multiple information domain architecture.....	31

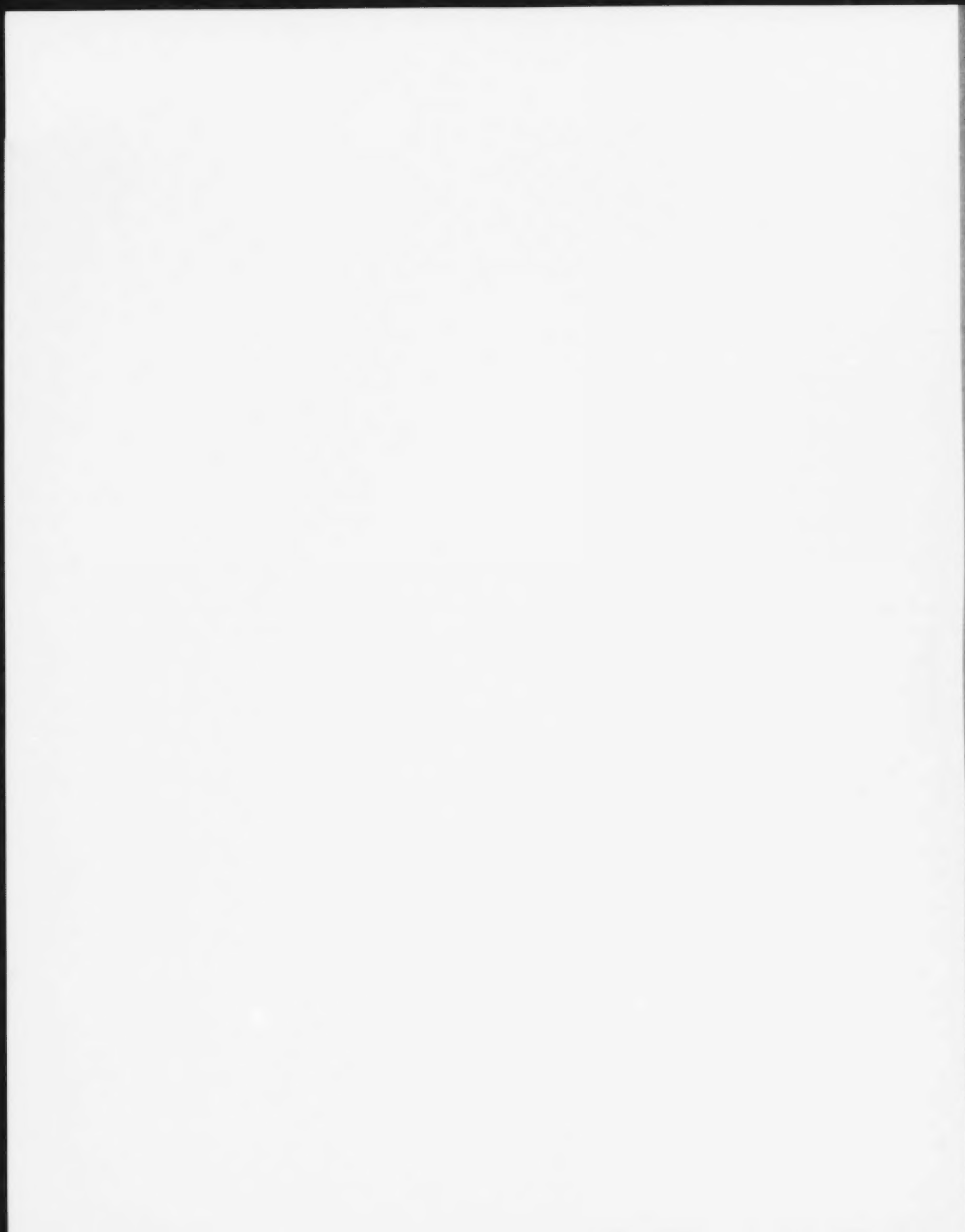
A.4 Generic CBIS architecture	32
A.4.1 CBIS networks and LSS nodes.....	33
A.4.2 Network encryption	34
A.4.3 Information objects.....	34
A.4.4 Information exchange mechanisms.....	35
A.4.5 Initialization and capability of LSS nodes	35
A.4.5 VPNs.....	36
A.4.6 Generic CBIS architecture: advantages and limitations	36
Appendix B: Presentation slides	40
Appendix C: Questions asked to stakeholders.....	75
Appendix D: Meeting Agenda.....	81

List of figures

Figure 1: Face partially hidden	12
Figure 2: A two SHE cluster.....	16
Figure 3: Linked clusters	16
Figure 4: Classical architecture for systems implementing an information domain.....	30
Figure 5: Generic CBIS Architecture	33
Figure 6: User-LSS node for CBIS ACTD	34

List of tables

Table 1: Advantages and limitations of the three architectures	39
--	----



1. Introduction

Given the resurgence of interest in Multi-level Security (MLS) and the advance of new technology and concepts, Defence Research and Development Canada (DRDC) Ottawa is organizing and leading a series of meetings on MLS intended to support the MLS needs of Canadian Department of National Defence (DND), the Canadian Forces (CF), and Other Government Departments (OGDs). The first meeting was held in February 2004 at DRDC Ottawa. The second meeting was held at DRDC Ottawa on April 6, 2005. This Memorandum documents the information presented and the results agreed in the second meeting.

The theme of the second DRDC Meeting on Multi-Level Security was short-to-medium term solutions for current MLS issues within DND, the CF, and OGDs. The meeting agenda is included in Appendix D. The twenty-five (25) participants attending represented the participation of the Network Information Operations (NIO) section of DRDC Ottawa, DND, the Collaborative Capability Definition Engineering and Management Demonstrator (CapDEM) project, the CF, OGDs, and DND contractors.

At the beginning of the meeting participants were asked to provide their objectives and expectations for the meeting. Section 2 presents this information.

Four presentations were then given. The abstracts, questions, responses, and comments related to presentations are found in Section 3. Furthermore, the presentation slides are provided in Appendix B.

The first presentation was on the Project Arrangement commissioned by The Technical Cooperation Program (TTCP) C3I to demonstrate network management across security domain boundaries in a coalition network consisting of three national coalition sub-networks, (Canada, US, and Australia). Each coalition sub-network is a national coalition security domains or simply a coalition domain. Each coalition domain is weakly linked to a higher classified national security domain on a national network. The management of the coalition network is coordinated by exchanging high level policies across the coalition domains boundaries to maintain a low bandwidth service and a quality of service across the coalition network. The project addresses the issue of cross-domain information management flows between the coalition domains and their national network domains: low-to-high information management flows are implemented through proxy mechanisms. The possibility of more extensive information flows between coalition and national domains were discussed during the question period. It was noted that this problem would be more difficult to solve for unstructured information but the project shows that some form of automated information exchanges between security domain of different classifications are possible.

The second presentation was on the Segregation and Hardening of Systems using Virtual Machines (VMs) presented by Cinnabar Inc. The VMs approach could replace MLS operating systems as a solution to provide an information sharing mechanism among many security domains. Information flow issues between virtual machines were discussed.

The third presentation introduced the usual security domain architecture that is based on an assignment of networks to security domains. The architecture was described through the concept of linked System-High Enclaves (SHEs). An architecture based on a single network was also presented. As an example of an architecture based on a single network, Appendix A describes the Generic Content Based Information Security (CBIS) architecture.

The last presentation was on the application of a facial recognition system developed at DRDC Ottawa to provide assurance that, at any time, a user logged onto a workstation is the same one that logged on originally. This is a low-cost solution that improves workstation security.

During the discussion session, participants were asked to provide their input on short-to-medium MLS solutions for a case study. Points covered were the domain architecture to be selected, characteristics of this architecture, and information flow control systems. Section 4 covers the material of the discussion session.

Six questions were asked to participants at the Wrap Up and final session. Appendix C gives the responses of the participants and Section 5 provides an analysis of the responses.

Finally, conclusions and recommendations are provided in Section 6 and 7, respectively.

2. Objectives/Expectations of stakeholders

Presented by Karim Dahel, NIO section, DRDC Ottawa

After general administration information on the meeting was provided, the meeting participants were asked to provide their objectives and expectations with respect to the Second DRDC Meeting on Multi-Level Security. The following points summarize their responses:

- Obtain the status of MLS research efforts in DRDC
- Present the CNMS project
- Understand the current state of MLS solutions
- Gain a better understanding of the state of MLS in the Government
- Investigate current local MLS research and development, with the intent of integrating MLS capabilities into ongoing and future projects
- Present Cinnabar's current R&D on the use of VM technology to provide an MLS solution
- Learn about MLS research status within DND
- Understand what MLS means to the end user
- Achieve an understanding of ML/CS requirements within the DND community
- Obtain more information on MLS designs and solutions from DRDC
- Determine DND stakeholders in ML/CS C&A process
- Learn of research and industry progress in achieving potential future MLS implementations. In doing so, obtain an updated view on current constraints and limitations
- Hold an educational workshop on the developments and vision of an MLS system and the issues that need to be addressed
- Gain insight and understanding into the fundamentals of the MLS problem, possible solutions, status of research and the progress being made to resolve the problem, the perceived timeline for operational deployment of initial solutions
- Obtain a general awareness of the current developments concerning MLS and short/medium term forecasted production capabilities
- Make stakeholder contacts for the ongoing Navy ML/CS evaluation
- Discuss the relationship between available MLS technology and people
- Understand the process and the inherent difficulties of implementing an MLS solution in the military environment

3. Presentations

Four presentations were given at the Second DRDC Multi-Level Security Meeting. This section provides abstracts of the presentations, the questions asked during the presentations, the answers to the questions, and related comments.

One of the selection criteria for the presentations was that they should address issues related to the control of information flow between security domains, because these issues are fundamental MLS issues. The first three presentations discussed such issues.

3.1 Presentation 1: MLM: Coordinating Network Management across Security Boundaries using Policy Resolution

Presented by David Kidston, CRC

3.1.1 Abstract

This talk describes issues dealt with in a recent TTCP C3I PA. This project examined questions such as: "What is the difference between a management domain and a security domain?", "How much information must pass between security domains to coordinate coalition-wide network management activities?", and "How can policy be used to integrate cross-domain network services including QoS management?". The lessons learnt from the multi-national policy-based management system developed by Canada, Australia and the US will be discussed, as will the follow-on work currently being pursued.

3.1.2 Questions from stakeholders and responses

- Q: Which is harder to share (regular) information or network management data?
- A: Regular information is much harder to share because it lacks the structure and other verifiable attributes that are inherently part of network management data. In the US portion of the PA work SNMP data and protocol parameters were verified by their management control interface (MCI) to insure that there were no covert channels and that only the management information cleared for release was downgraded to the coalition network.
- Q: Has any of the technology and policy work made its way into the operational environment, in any of the three participating countries?
- A: The US MCI is being, or has been, integrated with the ISSE guard. I'm not currently up to speed on the speed of their deployment.
- Q: Is this work finished or continuing? If finished, is a report available?
- A: The PA is now complete, and the meeting reports are available through standard TTCP channels. There is also an UNCLASSIFIED MILCOM 2004 paper [1] that

summarizes the work under the title "Distributed Multi-National Network Operation Centres."

- Q: Who sets the policies for the coalition assets?
- A: The coalition commander is ultimately responsible for the assets that have been loaned to the coalition.
- Q: How are policies combined or unified or separated?
- A: This is an active research area. In the PA we take a simple approach where policies are added together and the sum is either accepted or denied by the various parties involved in the coalition. Some kind of real time negotiation was discussed in the PA but was not implemented for the demonstration held in the fall of 2003.
- Q: Are conflicts within and between policies resolved? If so, how?
- A: This is another active area of research. In the PA the policies were designed to be non-overlapping. Each technology brought into the PA had a separate low level policy structure that was derived directly from the high level policy. Since there was no element of timeliness in the policies and all low level technologies had orthogonal duties, no conflicts could occur. In a more realistic scenario, where devices may have multiple functions, policy conflict resolution will be a critical part of the policy system.
- Q: When a piece of information is on the Coalition domain, can it be accessed by all National domains equally?
- A: In the case of network management information, no national network had access to the network common operational picture. It was, however, accessible to all coalition enclaves equally. In the scenario we chose, the national networks were sharing information with the coalition in order to aid the coalition commander in his duties.
- Q: What do policies look like? Based on any standards? XML?
- A: The policies we developed were written in XML and tailored for the technologies of the PA. It would be preferable to have natural language high level policy but this was not pursued.
- Q: What were the costs (hardware, software) associated with the coalition assets that had to be put in place?
- A: The demonstration, while complex, did not place an undue financial burden on the three research laboratories involved. Each lab provided on the order of 10 computers, about half of which were Windows-based, with the rest Linux and Solaris. Each also provided an IP Phone, HP Openview license and an ISDN link to

the other members. The rest of the software was open source or developed by the individual labs and provided to the others for their use during the PA.

3.2 Presentation 2: Segregation & Hardening of Systems via Virtual Machines

Presented by Eugene Basic, Cinnabar Networks Inc.

3.2.1 Abstract

Virtual machines offer a variety of innovative approaches for developing solutions to the hardening and segregation of systems. The use of virtual machines allows for the creation of rudimentary multi-level secure systems with each guest operating system residing within its own protected silo. These silos can be hardened to ensure that information from one does not accidentally spill over into another. Although the strength of each silo is insufficient, at the moment, to handle highly classified information, within fairly homogenous environments where users are cleared to the same level and yet must manipulate information at various classifications; this may offer a viable alternative.

Similarly, virtual machine architectures allow for the hardening of systems in innovative ways to ensure that the information within a given silo is further protected. In fact, the use of known hardening techniques coupled with cryptography and other technology can allow for the silos to be hardened against most common threats. Furthermore, hardening the system at the VM level allows for the centralized control and monitoring of the hardening so as to provide uniform hardening throughout an enterprise. The advantages and possibilities of this type of approach will be discussed.

3.2.2 Questions from stakeholders and responses

- Q: What investigation work has been conducted regarding possible C&A requirements and approaches?
- A: No investigation has been done, at the moment. This is purely a research focused task. However, the research is being conducted so that it could at a future date meet the requirements of the Common Criteria. As such it should meet certain aspects of C&A as well.
- Q: Can information be passed between VMs?
- A: At the moment some VM-based technologies allow for the movement of Information between operating images. VMware for one does this. However, work by NSA and VMware has provided means to disable the copy and cut-and-paste between VMs. Our design is to enable this feature thereby disallowing data movement between the VMs.

The corollary to this is can we allow trusted movement of data between the VMs? At the moment, no. However, one of the design goals is to allow for write-up and read-down based on rules governed via a centralized LDAP service. This, however, requires the creation of a strong engine controlling how the information moves. The initial thoughts in this area are to use a proxy-architecture whereby the proxy performs the movement on behalf of any given VM. Again, this is something we have only done a preliminary look into.

Q: What is the relation (similarities/differences) of Cinnabar efforts to those by NSA with SE linux and HP?

A: We're approaching the MLS problem from a different perspective than NSA and their SE-Linux initiative. Our goal is to utilize a minimal Linux kernel for all our work. We feel that in this way we can minimize the likelihood that there is something operating that can impinge on the security we're trying to attain. It also allows us to better control the system underpinning the VM technology. In effect, our view of the host OS is as though it was a hardware abstraction layer (HAL). And as such we want to minimize the number of changes and number of processes that are running to the bare minimum required. SE-Linux, on the other hand, approached the problem from the other end: creation of a general-purpose OS. Our belief is that the general purpose OS would operate on top of the HAL as a virtual machine image and, that each image would provide the end-user with an experience as close to what he or she was used to as possible. In other words, beyond some minimal initial security procedures, the user would utilize the computer and its operating system as though it were the only thing operating on said hardware.

The other major difference is in how we want to segregate information. Our goal is to place information within protected silos. Information placed within a silo automatically is of the classification of that silo. We don't assume that the user can or will be able to mix classification levels. If a piece of information is copied to the local image, it automatically is assumed to be protected in the same way as the information on that device. Although this latter point may not be optimal, the goal is to create a system that allows for multiple images at differing levels. With the ability to run multi-headed systems, you could have each system displayed on its own monitor alleviating some of the hassle this would cause.

The largest similarity between the two solutions is that neither offers a fully MLS-type system as described by many within the security field allowing for transparent, secure, simple MLS-type transactions at the desktop. We're trying to approach the problem in incremental steps with each step taking us closer to the Holy Grail that is MLS.

Q: There are two or three US vendors working on systems with separation kernels (Windriver, Green ?), and there is a product called PCIntegrity. Has this research followed the development of those?

A: No. We haven't looked at those. But thanks for the information.

Q: Is it possible for a user to have multiple VMs active on a single machine and be able to move information/data from one VM to another?

A: As per the cut/copy-and-paste issue, it is possible to copy between VMs. However, our initial goal is to create silos that disallow the copy-and-paste of information. However, we are looking at proxy-based abstractions that would allow for the safe movement of information between silos.

The problem of information motion is something that needs addressing. The use of meta-data may well be crucial to the proper and safe movement of information between silos. Furthermore, XML offers the best ability to wrap information with pertinent information. The problem of ensuring it remains with the information is another question, but one that is being addressed by the likes of Microsoft and Apple.

Q: What effort/testing has been conducted to provide assurance that the memory remains separate.

A: At the moment we are assuming that the protection offered by the chip would be sufficient. Of course this may not be sufficient. We are focusing on the problems at hand with respect to siloed data stores provided via the thumbdrives.

However, I'm unsure whether any MLS-style solution currently addresses this concern. Furthermore, I'm uncertain whether any MLS-style solution is sufficiently tied to the underlying hardware (most cases x86) to offer anything more than the standard memory management protection of the hardware. Back in the late 80s and early 90s CSE examined MMUs and found them to be sufficient for protecting memory from errant access. I'm not sure if this research was ever followed up, but as the chips then examined (680x0 and x86) are ancestors or the current chips, I would assume the findings remains true. At some point, as pointed out in each evaluation criteria, trust must be assumed. This is usually placed at the hardware level.

Now, if we move the problem upwards towards the memory management provided by the kernel, then we have another set of issues. As our goal is to hide the VM and the underlying OS from the user, it may be possible to achieve a lot of security through obfuscation and indirection. Strengthening the kernel may be necessary but it isn't something we're heavily looking into yet.

Q: If thumbsticks are connected to the "PB" guest, will a secondary thumbstick will be required for the "secret" guest? Or will encryption take care of data segregation?

A: At the moment we're opting for a separate stick for each data type. Research is preliminary and we want to keep the variables at a minimum. The ultimate goal is to utilize encryption as effectively as possible across all aspects of the solution. However, to keep it simple, initially the thumbdrive will be encrypted for a single classification level. Furthermore, the current design has each thumbdrive storing a resident VM image.

3.3 Presentation 3: Overview of some MLS architectures and MLS solutions

Presented by Jean Savoie, NIO Section, DRDC Ottawa

3.3.1 Abstract

The usual way information confidentiality is protected in classified security domains is through network separation. We will describe this domain architecture made of linked System-High Enclaves (SHEs).

A SHE is defined as an enclave (a secured physical location) composed of one or more networks in which each network is assigned to a security domain and provides an implicit labelling to the information it contains. In simple enclaves, there is no connection between networks other than those provided by air-gaps and procedures. Simple SHEs are easy to implement because they don't involve explicit labelling, complex information management, and IT infrastructure. However, they don't provide any automated information transfers from one network to another, which impedes information sharing. In more complex enclaves, networks are linked in a controlled manner. We will show many examples of such connections but all provide only partial solutions to the information sharing problem.

SHEs are linked together through VPN technology but only networks belonging to a same security domain are linked together: inter-domain information flows are controlled within SHEs or through SHE clusters. A SHE cluster is a set of SHEs that are physically close to each other.

There exist other domain architectures that don't involve many networks. We will talk briefly of CBIS, which is an example where information is separated by encryption (see also Appendix A).

Finally, an overview of the US Global Information Grid (GIG) will be provided. We will emphasize the new services that the GIG will support to provide a better information sharing capability. Some questions on the difficulty to achieve the GIG will be also discussed.

3.3.2 Questions from stakeholders and responses

Q: Is CBIS the same as CBAC?

A: No, CBAC means Content Based Access Control while CBIS means Content Based Information Security. CBAC is often implemented through intelligent agents searching for key words such as "Secret" or "Top Secret". The access control is based on those words. On the other hand, the main purpose of CBIS solutions is to separate information of different security domains. In all envisaged CBIS solutions the separation is through encryption, which allows a single network solution. For

instance, in the US CBIS Advanced Concept Technology Demonstrator (ACTD), each security domain has a domain key, which is used to encrypt keys that encrypt the domain's information objects. Hence, when a user in the domain wants to read an information object in his/her domain, he/she decrypts the object's encryption key obtained from a domain server and then decrypts the information object. In this ACTD, the only mechanism provided to exchange information is by exchanging encrypted files; so there is no teleconferencing mechanisms provided, for instance. However, there are no inherent limitations to such new mechanisms. For more information on CBIS, see Section 5 of [2] and Appendix A.

3.3.3 Comments from stakeholders

With an interactive diode low-to-high connection, it is technically possible to achieve high-to-low connectivity, however due to security policies, we do not allow it. Furthermore, using the VETO data diode example implemented on the TITAN network, from the DWAN to the C-NET, provides a capability for automated data stream transfer.

It is absolutely certain that the data diode will technically allow high-to-low information transfer. A great deal of effort was expended to achieve the ITSEC 6 certification. It may be that the 'dummy' connection on the VETO is used to appease the protocols being used (i.e. acks) rather than technically allowing a data flow in the opposite direction. The ITSEC 6 certification is an expensive undertaking to produce something that also doubles as a router.

In our context, we do not allow for high-to-low with VETO for policy reasons, and as you mention, certification, but technically, it does not matter to VETO on which side the high network is located. That is why we can say that it is technically possible for a VETO diode to take information from any side and send it across the other. However, as you mention, so far, a dummy VETO is coupled with the other one, to give it the "high" end communication protocol so the VETO can transfer data from low-to-high. With a real high network instead of a dummy VETO, information could flow in both directions, but we don't allow that to happen.

3.4 Presentation 4: A trusted user monitoring system with biometrics

Presented by Qinghan Xiao, NIO Section, DRDC Ottawa

3.4.1 Abstract

The ability to prevent unauthorized users from gaining access to sensitive or classified data is of crucial importance to government organizations. In recent years, there have been significantly increased interests in biometric technologies in order to enhance the security of physical and logical access controls. Generally, biometric technology can be used either for authentication or identification. Currently, once a user has logged on to a system; there is no mechanism to check if the user has left the workstation without logging off, leaving the system open to unauthorized users. It is important to ensure that the user, throughout the session, remains the same authorized user for all applications. To address this security

vulnerability, DRDC-Ottawa has developed a demo system that combines biometric authentication and monitoring functions. The system uses a fingerprint to authenticate a user. After the user has been successfully authenticated, face detection and face tracking functions are performed to monitor the user. The PC will automatically log off when the authenticated user's face disappears for an adjustable time interval. This demo system will be further developed in the next step to include facial matching function. The final system can be used in high security environment to ensure that the user at the workstation is always the same authenticated user.

3.4.2 Questions from stakeholders and responses

Q: Can the camera be fooled by a photo?

A: Yes, at the moment the system only works on a 2D image. It could distinguish a 3D face from a 2D (flat) image if we add another Webcam and process stereo images.

Q: What about privacy issues?

A: As to the face monitoring feature, the privacy issue is minimum because we are not using the face recognition to authenticate, but only monitor the users. The first face image will be captured after a successful authentication. All the face images can be deleted after a user has logged off.

Q: What happens if you hold a phone to your ear?

A: The system recognises you even if the user's face is partially hidden by a small-to-medium object.

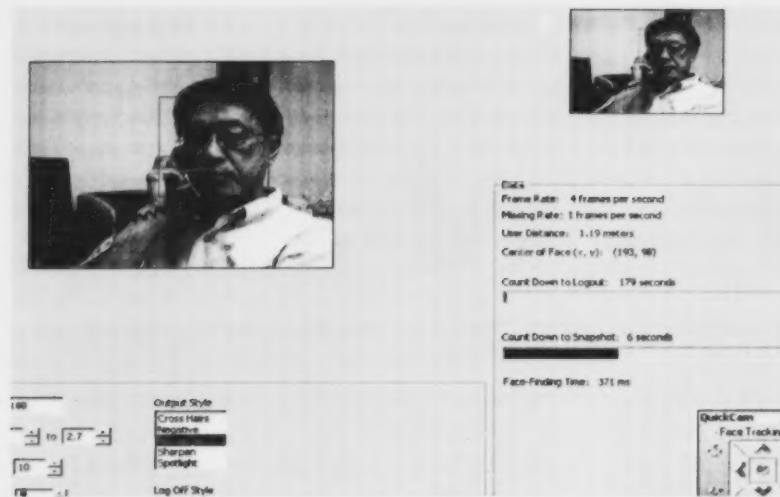


Figure 1: Face partially hidden

4. Discussion session

The objective of the session was to discuss MLS issues that have short-to-medium term solutions. The session started with a discussion of the characteristics of the current Information Assurance (IA) architecture because short or medium term solutions are more likely to be built from current solutions. Then, the notion of a classified network was defined and discussed. Finally, a case study was presented for which a MLS solution was desired. Two solutions were presented and discussed.

4.1 Characteristics of the current IA architecture

Dr. Savoie presented some characteristics of the current IA architecture, which were discussed during the session. The current IA architecture can be approximately seen as a set of linked enclaves.

4.1.1 Enclave characteristics

- Enclaves are composed of one or more networks weakly connected. Classified enclaves are physically protected and have a well-defined physical boundary.
- Enclaves are System-High enclaves: All users are cleared for all information inside the enclave
- Enclaves with many networks use physically separate networks to separate information. Hence, networks provide implicit labelling for information. Too often networks support a single security domain. In simple enclaves, networks are disconnected and procedural mechanisms involving a man-in-the-loop are used to transfer information from one network to another. While networks are connected, filtering and procedural mechanisms are used to transfer information from network to network (see Presentation 3 in Appendix B)
- Networks in enclaves are usually red (i.e. no IPsec or HAIPE encryption). Internal threats are often assumed to be low
- Remote users access enclaves through firewalls, guards, or special access servers entry points.
- Workstations in enclaves are often standard workstations that are not well protected physically by themselves and are subject to trojan horses and spy software
- Enclaves are linked to form enterprise networks. They are linked using VPNs that connect networks belonging to the same classification or security domains. VPNs are few. Large scale VPN systems are complex to manage and labour intensive.

4.1.2 Information Management characteristics

- Information management is limited. It is difficult to retrieve and share information if the information and the users are not in the same security domain. There are few information sharing mechanisms.

- Information domains (security domains, classified domains) are logical entities that correspond often to physical entities. (e.g. a classified network becomes the physical entity corresponding to a classified domain logical entity)
- No electronic labelling of information

4.1.3 Why classification of networks is useful

Classifying information assigns a value to the information with respect to confidentiality, and possibly also with respect to integrity and/or availability. It is not always clear to which terms the value of an item of classified information applies. In some contexts, only the confidentiality value is considered while in others the integrity and availability values are very important.

Classifying a network involves the following:

- Bounding to the value of the information on the network to no more than the network classification, and
- Stating that the network users are cleared to access all information in the network, assuming System-High mode. Note that need-to-know is usually assumed in classified networks, so users cannot actually access all information on the network.

Classification of networks allows the organizations managing them to provide core security policies and standard protection mechanisms for confidentiality, integrity, and availability of information. Even though organizations provide security policies and standards, not all classified networks of a same classification are equal. So, it is necessary to add protection to some networks depending on their particular characteristics. This shows that assigning a classification to a network is equivalent to assigning an attribute to a network that incompletely specifies the security measures to be applied to protect the network. Is it possible to add more attributes that would completely specify the security measures to be applied? This is probably a subject for research.

Current security policies and standards for classified networks provide sufficient physical security measures to allow red networks in enclaves, standard workstations, and simple authentication/authorization mechanisms inside enclaves. Moreover, clearance of the personnel and their limited number are often strong arguments for considering internal threats to have a low probability.

4.2 A case study: CapDEM

The Collaborative Capability Definition Engineering and Management (CapDEM) process demonstration project was considered as a case study for determining an MLS solution applicable to CapDEM.

4.2.1 CapDEM's mission

The CapDEM mission is to provide a common decision-supporting process accessible by many organizations and partners and an environment to support senior defence decision-

makers in the development of capabilities. It also provides a tool for dealing with the challenge of analyzing/developing solutions to military capability gaps.

4.2.2 CapDEM's MLS objectives

The MLS objectives of CapDEM are to manage information that includes

- commercially sensitive IP (i.e. proposed solutions to DND capability gap RFPs);
 - unclassified;
 - SECRET CA/US details on current capability gaps, and
 - TOP SECRET CA/US details on current capability gaps
- in a central repository accessible from many partners of different classifications.

4.2.3 CapDEM's assumptions

CapDEM's assumptions are the following:

- Information classification levels up to Secret,
- A central information repository, and
- An distributed environment.

4.2.4 Solution 1: Linked System-High Enclaves (SHEs)

Linked System-High Enclaves (SHEs) was proposed as a possible solution (see Presentation 3 in Appendix B for more information on SHEs). CapDEM would be a set of linked SHEs grouped by clusters made of two SHEs. The following figure shows an example of such cluster. Each SHE contains a single network. One SHE contains an unclassified network while the second SHE contains a secret network. These two SHEs are physically close to each other to allow manual transfers of information from one network to another. Time limitation didn't allow the participants to discuss possible automated mechanisms and procedures for information transfers that support the CapDEM business processes.

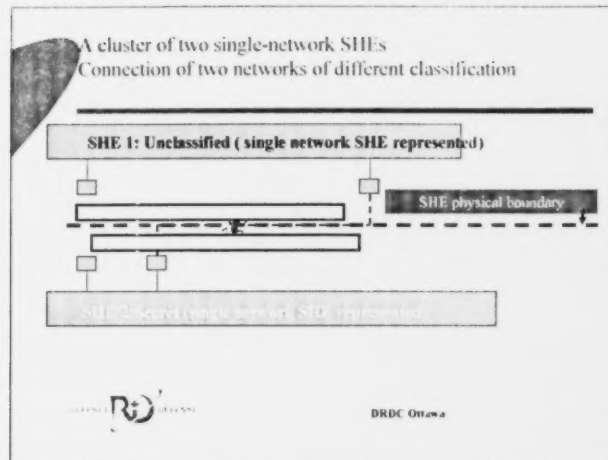


Figure 2: A two SHE cluster

The following figure shows how clusters would be linked together. Networks in different clusters are linked together only if they have the same classification. This is done by VPN or NEU technology.

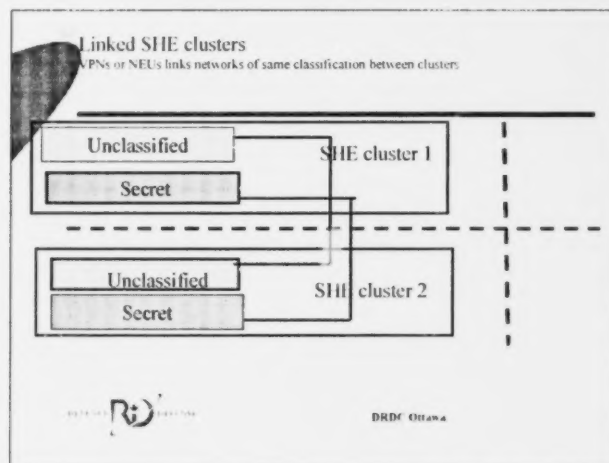


Figure 3: Linked clusters

Many issues were not considered. For instance, does CapDEM desire to provide remote access? Is the Secret network separated into security subdomains (caveat separation)? If so, how can this be implemented?

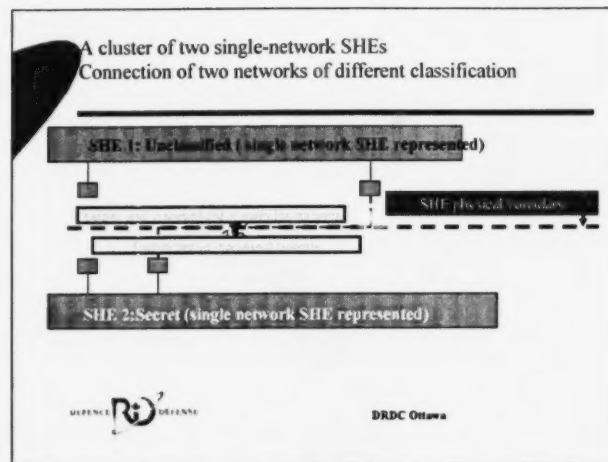


Figure 2: A two SHE cluster

The following figure shows how clusters would be linked together. Networks in different clusters are linked together only if they have the same classification. This is done by VPN or NEU technology.

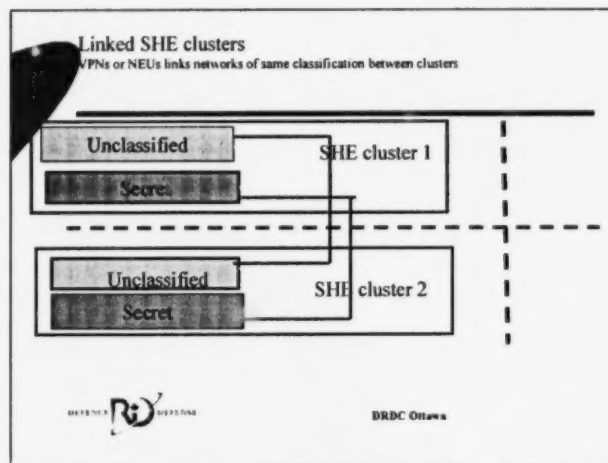


Figure 3: Linked clusters

Many issues were not considered. For instance, does CapDEM desire to provide remote access? Is the Secret network separated into security subdomains (caveat separation)? If so, how can this be implemented?

4.2.5 A single network solution

Only few minutes were spent discussing this solution. This solution could be based on the separation of information through encryption mechanisms as envisaged by the US CBIS ACTD or as described in [2] and Appendix A. However, if such a solution is envisaged it would be necessary to label information electronically.

5. Wrap up session

During the wrap up session, several questions were posed to the participants. The answers are documented in Appendix C and analysed in the sub-sections below.

5.1 What is the single most important problem to be addressed by an MLS solution in immediate term? What is the most promising technology to begin implementing a solution in the short term?

The problems defined by the participants can be grouped in four classes:

- Certification and Accreditation
- Multi security domain solutions
- Labelling
- Definition of business processes

Each class is analysed in the sub-sections below and the associated technologies are described. Participants also expressed the need for a working group that would be interested in MLS or multi security domain solutions. Good solutions involve acceptable costs and interoperability with COTS products.

5.1.1 Certification and Accreditation

Policy and procedures for the use of MLS need to be changed. Accreditation criteria and security policies to allow for MLS need to be reviewed in the light of the need to share information across security domains. At the recent DND Enabled Operations Symposium and Workshop held in Ottawa, November 30 to December 2, it was determined that people, more than anything else, were the bottleneck. It is the same for MLS. MLS proofs-of-concept could be developed in spite of current policies. However, it is necessary to understand the rationale for the current policies to make sure that these proofs-of-concept involve good design principles that mitigate the risk to an acceptable level.

5.1.2 Multi security domain solutions

Multi domain solutions can be small or large systems. Small systems could be workstations able to access many security domains of the same or different classifications. They may have limited data sharing capabilities. Workstation solutions could be implemented through MLS workstations or virtual machines. More larger systems could involve data diode, guards, web and mail servers, etc. Examples of complex solutions are discussed in Section 4 and Appendix A.

5.1.3 Labelling

Information labelling needs to be addressed. Encapsulation of information to provide simple, immediate tagging of information to assist in the creation of MLS solutions can be a simple solution. Such tagging solutions could be easy to implement but would have only

local value: non-local systems may not support the tagging. Currently, labelling issues are addressed often through implicit labelling. For instance, networks are often used for that purpose.

5.1.4 Definition of business processes

The definition of business processes that we would like to protect and automate is needed. The lack of business process definitions is probably one of the reasons why MLS problems are so hard because people want MLS solutions that are independent of business processes. A better approach to MLS solutions would be to design them for classes of business processes.

5.2 What would be the most promising MLS research areas in term of value for DND?

Only three areas were identified: High-to-Low data transfer, trusted computer base, and data aggregation. All involve information flows controls. The limited number of answers is probably due to the fact that participants provided examples of research areas in answers to the two previous questions.

5.3 What are the most important issues to be addressed at the next meeting?

The most important issues for a next meeting on MLS were the following:

- A report on any progress made, including the current state of the art for MLS, assuming it has moved forward in six months to a year.
- A report on new MLS technologies available and the state of our allies with respect to MLS.
- Certification opinions on various multi-caveat/multi-level security approaches. Unclassified level certification (e.g., Common Criteria), as well as input on High Assurance evaluation approaches (required for a classified solution)
- Discussion of concrete issues that can be applied to (a) real solution(s), rather than just a discussion of the problems.
- Problems encountered with development.
- Development of business requirements. There was a great deal of work done in the '70s and '80s, and some in the '90s that needs to be reviewed. DRDC Ottawa and CSSC (CSE) both did extensive work, as did NIST and NSA.
- Are there any accepted architectures for MLS that have evolved from current research?
- Industry initiatives: An industry day could be hosted on the subject with syndicated discussion between DND and industry on specific issues.
- Establish a database on works done with respect to MLS or information domain separation within DND and OGDs, or, at least a single web page to visit with all the necessary links.

5.4 What are the characteristics of the Certification & Accreditation process? What would be the characteristics of a better C&A process? How can this be implemented?

The C&A process for a system evaluation was described in the following simple terms: A system evaluation is a risk evaluation of the system. If the risk is acceptable to the control management, then someone signs to accept the responsibility. If the risk is not acceptable, the C&A people may suggest some safeguards or ask for undefined modifications to the system.

It was not clear from the discussions and answers whether or not the preceding paragraph is an accurate description of the C&A process. It is highly probable that a system evaluation involves more than just a risk evaluation. This issue is open for further clarification.

A risk evaluation of a system is usually based on sensitivity of the information processed by the system, the threat environment, system vulnerabilities, and IT, physical, or procedural safeguards. Some other elements may be also be involved. On the other hand a system evaluation is based on a risk evaluation, security policies, and possibly other elements such as Common Criteria and best engineering practices. It is shown in this section that securities policies relate to elements not involved in risk evaluations. This will show that system evaluations are more than risk evaluations. Furthermore, the roles of security policies and the way they can be developed are discussed. Finally, other elements of system evaluations and risk methodology are discussed.

5.4.1 Roles of security policies in system evaluation

Security policies have a security role in system evaluations but may also have other roles, such as interoperability. For example, assume that the statement "Type I crypto needs to be used in a classified network for encrypting information" is a security policy used for a system evaluation. This policy has at least two roles: interoperability and security.

Roles need to be known and explicit; otherwise, new systems would be denied certification for the wrong reasons. For instance, a crypto system might not be certified only for an interoperability reason even though it provides an acceptable risk and has no interoperability needs. So the knowledge of the roles of a security policy may help evaluators in defining new security policies that are more appropriate when the context changes.

5.4.2 Security policy context

The security role of security policies can be seen as a safeguard against a set of threats. Since these threats are not normally enumerated, they are implicit. The fact they are implicit is a problem. Originally, some security policies have been set in a context that is assumed to be technology-and-procedure dependent. This means that the safeguards provided by the security policies are a set of safeguards for a given technology and

standard procedures and these security policies must be seen within a security context. The notion of explicit security context should be important to policy makers: they will be able to reuse work done from existing security policies.

5.4.3 Rationales of security policy contexts

Risk evaluation should be based only on risk, not on security policies. Nevertheless, security policies may simplify system evaluations. In addition, they can provide high level descriptions of acceptable safeguards, which can help designing acceptable solutions. So, security policies can be useful. However, they should not be seen as fixed. New security policies may be needed. How can one build new security policies? From scratch? Probably not! A better approach would be to get a context rationale for each security policy. This rationale could contain information on the environment where the policy is to apply, the explicit threats that are considered, and possibly other elements. Hence, policy rationales could then be reused to make new policies.

5.4.4 System evaluation versus risk evaluation

It has been shown in this section that security policies introduce elements outside of the risk evaluation into the system evaluation. It is important that the roles of security policies be stated. Moreover, policies should be accompanied by a rationale, to make it easier to define new security policies that are necessary when new technology becomes available.

5.4.5 Other elements of system evaluations

Systems are evaluated through a variety of criteria and best engineering practices. It may be possible to map these criteria and practices to elements of a risk methodology. However, no current methodology is known that does this. Such a mapping would be useful because the system evaluation would then be independent of the assumptions underlying these criteria and best practices.

5.4.6 Risk evaluation methodology

An efficient, fast, cogent risk evaluation methodology that is consistent among departments and organizations is needed. Moreover, estimators to measure the quality of risk methodology are needed. Without these estimators, the confidence on the measure of the risks is low.

6. Conclusions

MLS and multi security domain certifiable solutions are needed for many business or operational processes within DND and CF. These solutions should reduce risk to an acceptable level and address issues of information sharing and costs. Example of solutions could be the following:

- multi-caveat separation systems on classified networks;
- desktops accessing multiple security domains concurrently or sequentially;
- MLS workstations or virtual machines;
- high-to-low systems and guards;
- web servers for cross-domain information sharing;
- large IT systems based on the linked SHE or CBIS architecture in which new sub-systems are to be developed; and
- systems comprising IT systems, human procedures, and information management allowing execution of business or operation processes involving information from many security domains.

Since these solutions need to be certified and accredited, they should be developed in concert with C&A authorities. Certification is mainly based on risk evaluation and policies. Risk evaluation involves risk methodologies, while policies are based on rational arguments. So, the certification of systems is dependent on these methodologies and arguments. This may impede the development of new solutions if methodology and policies are fixed forever. Therefore, developers and C&A authorities need to work together to change methodologies and policies to allow the development of unforeseen solutions.

It may be impossible to develop multi-domain solutions that are good in all environment contexts. Systems involving IT systems, human procedures, and information management are such solutions. So, descriptions of environment profiles probably need to be developed. Environment profiles could include descriptions of operational or business processes; how information is organized, processed and managed; and a definition of user roles and sub-system roles. Some (partial) profiles may already exist in some form. Military and operational organizations may be of great help for developing these profiles that would allow certification work reuse.

Finally, as stated in Section 5.4, research areas in system and risk evaluations may be necessary to allow the definition of new security policies and the development of new multi security domain solutions.

7. Recommendations

The principal recommendation from the 2nd MLS meeting, after analysing the points raised and the discussions is:

To create a formal government-wide Multi Security Domain working group (WG).

This WG should involve the following departments and organizations:

- government C&A organizations;
- research organizations;
- Canadian Forces;
- DND engineering branches;
- DND contractors; and
- OGDs.

The scope of the WG would include the following:

- developing systems implementing automated or semi-automated business processes involving information from many security domains. MLS systems or systems supporting multiple caveats are examples of such systems. A system here can be very general. For instance, a simple system could be a workstation supporting a MLS OS or virtual machines while a complex system could be a set of networks linked by sub-systems along with a set of procedures that regulate users and information flows;
- describing CF or DND business processes involving information from many security domains;
- developing concepts useful to support multi security domain systems; and
- certifying and accrediting multi security domain systems.

It is recommended that the WG focus primarily on short-to-medium-term certifiable systems that can be implemented within limited resources and be useful to DND. In order to design, develop, and/or implement an example of such systems, the WG could initially determine a case study involving many security domains for which a solution useful to DND is needed. Then, the WG could try to find certifiable solutions. It is recommended that the WG include people from DND and/or CSE involved in C&A; otherwise, solutions may not be certifiable. Moreover, foundation work on security concepts along with their relationships may be necessary. For example, the concepts of security domain and Threat and Risk Assessment (TRA) are used to provide, respectively, a logical boundary to information objects and an evaluation methodology to systems. Therefore, the

determination of relationships between these two concepts could be a WG research area. Information provided in Section 5.4 could be used for that purpose. Another example would be to test if the notion of environment profile discussed in the conclusion could be useful to C&A personnel and system developers.

References

1. George, P., Kidston D., and Scott S. Distributed Multi-National Network Operation +- Centres. MILCOM 2004 conference paper.
2. Savoie, J. (2004). A strong three-factor authentication device: Trusted DAVE and the new Generic Content-Based Information Security (CBIS) architecture (DRDC Ottawa TM 2004-198).
3. Detombe J., Cowan D., Smith M., and O'Brien J. (2004). Survey of Multi-level Security (MLS) Products (DRDC Ottawa CR 2004-268).
4. Technical Architecture Framework for Information Management (TAFIM), DISA, <http://in.disa.mil/tafim.html>

8. List of acronyms

ACTD	Advanced Concept Technology Demonstrator
C & A	Certification and Accreditation
C2IS	Command and Control Information System
C3I	Command Control Communications and Intelligence
CA	Canada
CapDEM	Collaborative Capability Definition Engineering and Management Demonstrator
CBAC	Content Based Access Control
CBIS	Content Based Information Security
CCEP	Commercial COMSEC Endorsement Program
CF	Canadian Forces
CFCS	Canadian Forces Command System
C-NET	Classified NETwork
CNMS	Coordinating Network Management System
COTS	Commercial Of The Shelf
CSC	CBIS Security Card
CSE	Communications Security Establishment
DEA	Drug Enforcement Administration
DND	Department of National Defence
DRDC	Defence Research and Development of Canada
DWAN	Defence Wide Area Network
EAL	Evaluation Assurance Level
FC	Forces canadiennes

GIG	Global Information Grid
GSP	Government Security Policy
HAIPE	High-Assurance Internet Protocol Encryption
ISDN	Integrated Services Digital Network
IP	Internet Protocol
IP	Intellectual Property
IPsec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LSS	Local Sub-System
MCI	Management Control Interface
MDN	Ministère de la défense nationale
ML	Multi Level
MLS	Multi-level Security
NEOps	Network Operations
NEU	Network Encryption Unit
NIO	Network Information Operations
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OGD	Other Government Department
OS	Operating System
PA	Project Arrangement
PC	Personal Computer
PKI	Public Key Infrastructure
QoS	Quality of Service

R & D	Research and Development
RDDC	Recherche et développement pour la défense Canada
RFP	Request For Procurement
SHE	System-High Enclave
SNMP	Simple Network Management Protocol
TAFIM	Technical Architecture Framework for Information Management
TRA	Threat and Risk Assessment
TTCP	The Technical Cooperation Program
VPN	Virtual Private Network
VM	Virtual Machine
WG	Working Group

Appendix A: Generic CBIS architecture defined and compared

This Appendix is a modified excerpt of Section 5 of document [2]. It introduces some definitions and concepts related to information domains and their implementations; provides a short overview of the traditional architecture for systems implementing one or more information domains; and, describes the Generic CBIS architecture for systems that support multiple information domains. Furthermore, it presents advantages and limitations for each of these architectures.

A.1 Definition of information domain

Below is the definition of information domain provided by the Technical Architecture Framework for Information Management (TAFIM) [4]. Information domains are also called security domains in the literature and this document.

An information domain is a set of users, their information objects, and a security policy. An information domain security policy is a statement of the criteria for membership in the information domain and the required protection of the information objects.

Information objects can be transferred between two information domains only in accordance with established rules, conditions, and procedures expressed in the security policy of each of them.

The transfer can be accomplished only by a user who is member of both the sending and receiving information domain policies and, if required by the information domain policies, has been granted the appropriate privileges (e.g. "release authority").

Hence, an information domain security policy states the required protection of the information objects. Statements of security policies vary from policy to policy. Some require a security model for the system implementing the information domain. Security models have been developed to protect information from different types of attacks. Examples of well-known security models include the Bell-Lapadula model and the non-interference model.

A.2 Traditional architecture for a single information domain

The traditional architecture for a system (along with its environment) implementing a single information domain is shown in Figure 5. The system is composed of different red LANs connected together through a VPN. Each LAN is composed of connected workstations, servers, routers, and possibly other types of network nodes. The VPN is usually implemented through firewalls or Network Encryption Units (NEUs). The

information domain's users are the authorized users and they are the only ones that are authorized to logically access the system. Physical access to the system is restricted. For instance, authorized users cannot usually access servers, routers, and boundary controllers. However, they can logically access the system through entry points that are usually workstations. These workstations may or may not physically protected.

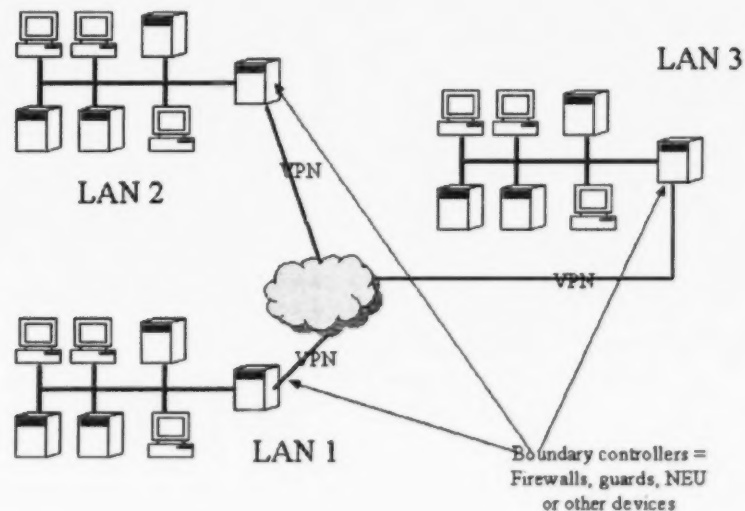


Figure 4: Classical architecture for systems implementing an information domain

There are a number of advantages and limitations of such systems:

Advantages:

- A1) Physical protection. The system's physical environment enforces the protection of information objects from physical attacks made by unauthorized users that do not have physical access to the system.
- A2) Logical protection. Firewalls/NEUs enforce protection of information objects from logical attacks made by non-domain users.
- A3) Security model based. The system can easily satisfy/implement security models such as Bell-Lapadula and non-interference because only one information domain is involved.

Limitations:

- L1) No automated inter-domain exchange mechanisms. Such a system does not allow any automated information object exchanges between the information domain implemented by the system and any other information domain.

L2) High hardware and management costs. Two systems and networks are needed to implement two information domains. This implies high costs.

L3) Confidentiality/integrity/authentication weaknesses. Such systems do not necessarily provide

- Confidentiality/integrity protection of information while information is in transit within the LANs.
- Strong authentication mechanisms to prevent logical access to unauthorized users that have physical access to LANs.

A.3 A multiple information domain architecture

The system architecture shown at Figure 5 is modified as follows to become a multiple information domain architecture:

Firewalls/NEUs become guards. Each guard is a multiple information domain machine that enforces the inter-domain flow control sub-policy of an information domain. The information domain is said to be the guard's information domain. The sub-policy controls the automated information flow from and to the domain.

All information objects that are located on a given LAN belong to a single information domain, which is the guard's information domain. Therefore, a LAN without its guard supports a single information domain. This domain is also said to be the LAN's information domain.

The architecture has the following advantages and limitations:

Advantages:

A1) Physical protection.

A2) Logical protection.

A4) Automated inter-domain exchange mechanisms. Transfers of information objects between domains are now possible.

Limitations:

L3) Confidentiality/integrity/authentication weaknesses.

L4) Guard implementation problem. It is difficult to implement such guards.

L5) Security model problem. It is not clear if it is possible to design a guard implementing a known security model.

L6) Single information domain support for LANs. Two LANs are necessary to implement two information domains.

A.4 Generic CBIS architecture

The system architecture shown in Figure 5 is modified as stated below to become the Generic CBIS architecture. Figure 6 shows an example of resulting system architecture. The security in this architecture is no longer based on physically separate networks but on protecting the information according to its content. There is no need to assign an information domain to each LAN: security is based on encrypted communication channels and encryption at origin (nodes).

The following points describe briefly the Generic CBIS architecture. These points are analysed in Sections A.4.1-A.4.6. Section A.4.7 states the architecture's advantages and limitations.

Elements of the Generic CBIS Architecture:

- **Network and specialized nodes.** The network is a set of connected nodes that are either supporting nodes, or Local Sub-System (LSS) nodes. LSS nodes are sub-systems composed of two or three nearby inter-connected physical components: a security card, an end-system, and possibly an authentication terminal. Note that Figure 6 needs to be interpreted in the context of the Generic CBIS architecture. The represented nodes are the LSS nodes and some supporting nodes. Boundary controllers and some other nodes can be either LSS nodes or supporting nodes depending on the CBIS architecture considered. In Figure 6, the boundary controllers shown are LSS nodes. However, they could also be simple supporting nodes (firewalls/NEUs)
- **Encrypted network communications.** Communications between LSS nodes are network encrypted with network keys.
- **Encrypted information objects.** Information is stored in information objects that are always encrypted outside LSSs. Information objects are encrypted by object keys, which are encrypted by group keys. There exists a one-to-one mapping between information domains and group keys. A user can access an information object in the clear only if the object belongs to an information domain to which the user also belongs.
- **Information exchange mechanisms.** Mechanisms exist to allow intra-domain information exchanges. Inter-domain information exchange mechanisms may be present, as well. Different types of LSS nodes may implement these mechanisms.
- **VPNs .** VPNs can be implemented by firewalls/NEUs.

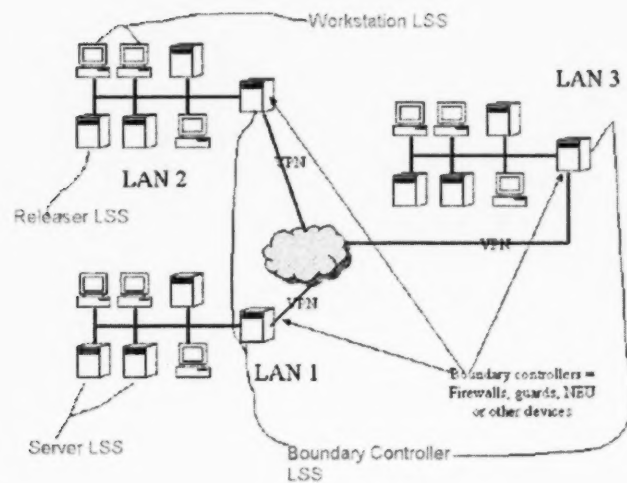


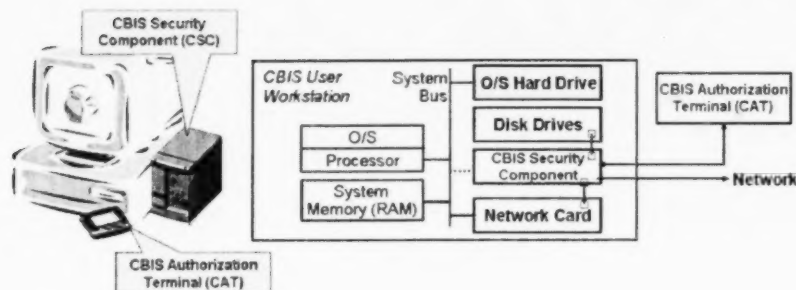
Figure 5: Generic CBIS Architecture

A.4.1 CBIS networks and LSS nodes

A CBIS network is a set of connected nodes that are either supporting nodes, or LSS nodes. A router is an example of a supporting node, while LSS nodes are sub-systems composed of two or three nearby inter-connected physical components: a security card, an end-system (e.g. computer or workstation), and possibly an authentication terminal. Therefore, workstations, and usually servers, or other types of end-systems are no longer network nodes; they are components of LSS nodes.

The security card is uniquely the LSS's external interface to the network; other LSS's components are attached to it. The main roles of the security card within an LSS are to perform network and object encryption/decryption, and securely store keys and credentials. Hence, the security card performs operations for which the end-system is deemed insecure. This is particularly true for user LSSs, which are defined below, because workstations are deemed insecure for the storage of keys and credentials and for authentication.

Different types of LSSs are possible. There are user and server types and some special types such as guard and releaser types. A type is associated with a functionality. For instance, an LSS that has the guard functionality is a guard type. Not all types are necessarily present in a given implementation. However, all implementations of the Generic CBIS architecture have user-LSS nodes, which are the nodes from which users work. In all implementations we assume the following: each user-LSS node contains an authentication terminal; end-systems in user-LSS nodes are workstations; nodes of other types may or may not contain an authentication terminal depending of the architecture's implementation. The following figure shows a user-LSS node envisaged for the CBIS ACTD.



- User LSS's components:
 - CBIS Security Component (CSC)
 - CBIS workstation
 - CBIS Authorization Terminals (CATs)

Figure 6: User-LSS node for CBIS ACTD

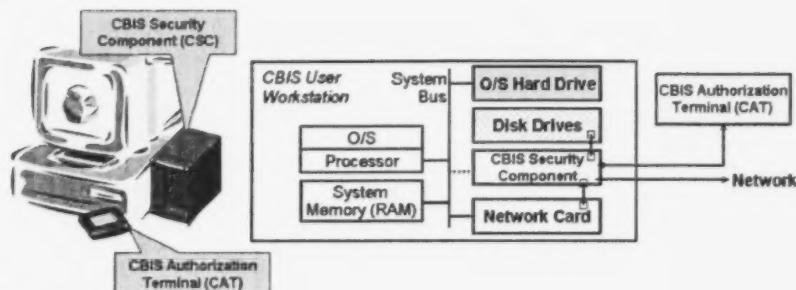
User-LSS nodes are multi-single-user secure nodes. This means that many users can use the node but at different time. Implementation of this could be made through period processing, MLS OS, or virtual machines. Normal users interact with the system only through user-LSS node. This interaction is through an authentication terminal for authentication and through a workstation for other purposes. Finally, in some implementations of the CBIS architecture, workstations have no hard drives or static memory directly connected to them to mitigate the risk of unauthorized information flows between workstation's sessions. Fig. 7 shows an example of such workstations.

A.4.2 Network encryption

All communications between LSS nodes are network encrypted with network keys. It is possible that some non-LSS nodes can be part of the network encryption system. Therefore, the network encryption system is not necessarily dependent on the object encryption system introduced below. For LSS nodes though, we assume that network encryption is performed and protected by security cards. Examples of systems providing network encryption are IPsec or HAIPE systems.

A.4.3 Information objects

Information is stored in information objects. An information object is object encrypted with an object key (e.g. a symmetric key), which is encrypted by one or more group-keys (e.g. a public key or a symmetric key). There exists a one-to-one mapping between information domains and group-keys. Encrypted object keys are bound with their respective encrypted information objects. Note that only LSS nodes are allowed to encrypt/decrypt information objects.



- User LSS's components:
 - CBIS Security Component (CSC)
 - CBIS workstation
 - CBIS Authorization Terminals (CATs)

Figure 6: User-LSS node for CBIS ACTD

User-LSS nodes are multi-single-user secure nodes. This means that many users can use the node but at different time. Implementation of this could be made through period processing, MLS OS, or virtual machines. Normal users interact with the system only through user-LSS node. This interaction is through an authentication terminal for authentication and through a workstation for other purposes. Finally, in some implementations of the CBIS architecture, workstations have no hard drives or static memory directly connected to them to mitigate the risk of unauthorized information flows between workstation's sessions. Fig. 7 shows an example of such workstations.

A.4.2 Network encryption

All communications between LSS nodes are network encrypted with network keys. It is possible that some non-LSS nodes can be part of the network encryption system. Therefore, the network encryption system is not necessarily dependent on the object encryption system introduced below. For LSS nodes though, we assume that network encryption is performed and protected by security cards. Examples of systems providing network encryption are IPsec or HAIPE systems.

A.4.3 Information objects

Information is stored in information objects. An information object is object encrypted with an object key (e.g. a symmetric key), which is encrypted by one or more group-keys (e.g. a public key or a symmetric key). There exists a one-to-one mapping between information domains and group-keys. Encrypted object keys are bound with their respective encrypted information objects. Note that only LSS nodes are allowed to encrypt/decrypt information objects.

A user can decrypt an encrypted information object only if the user belongs to an information domain for which the information domain's group-key can decrypt the object's object key.

A.4.4 Information exchange mechanisms

Different information exchange mechanisms can be implemented but the mechanism chosen depends on the capability of the LSS nodes involved. The capabilities of LSS nodes are related to their components and their initialization. This will be the subject of the following section. There are two types of LSSs: those that can encrypt/decrypt objects and all others. The first type is said to be of type O while the other is of type N. Note that all LSS nodes can network encrypt/decrypt. So, all type O nodes are of type N.

We may now consider different exchange mechanisms. Only three cases are considered here. The first two exchange mechanisms provide intra-domain information exchange examples while the last provides an inter-domain information exchange example.

Case 1: No direct exchanges between LSSs of type O. This is used by the CBIS ACTD. Information from an LSS node of type O is sent to/received from a node of type N. The node of type N serves as a repository: it cannot decrypt/encrypt information objects. In order for users to exchange information, they must belong to the same information domain and communicate through the repository.

Case 2: Direct exchanges between LSSs of type O. A communication link is set between two nodes of type O belonging to a same information domain. The information is first object encrypted and then network encrypted at a node to be sent to the other node, which can get the information by decryption.

Case 3: Information exchanges through a releaser LSS. In this case, a user sends information from an information domain to another. It is assumed that the releaser LSS can encrypt/decrypt object keys from the two information domains. The user sends information from a user LSS (type O) to a releaser LSS (type O). The releaser then decrypts the object key and encrypts it with the second information domain's group-key. Therefore, any user from the second domain may now get the information from the releaser's LSS.

A.4.5 Initialization and capability of LSS nodes

There are two types of initialization: the initialization of LSSs with an authentication terminal and those without an authentication terminal. All LSSs with an authentication terminal are of type O, while the others may, or may not be of type O.

If an LSS does not have an authentication terminal, the security card initializes its network encryption function. This can be implemented in several ways. For example, the credentials needed to perform encryption and negotiate session keys can be loaded dynamically from a server or loaded manually. Normally, these LSSs are not able to encrypt/decrypt information objects because they cannot decrypt object keys. This is the

case for server-LSS nodes. However, it is possible that other types of LSSs without an authentication terminal be type O node if they use embedded credentials to get authorization information and/or group keys from a key-server LSS.

If an LSS has an authentication terminal, the initialization can be performed in one or two phases. If it is performed in two phases, the first phase initializes the LSS's network encryption function as done in the previous paragraph. The second phase occurs when the LSS authenticates a user. The authentication terminal gets the user's credentials (e.g. PIN, fingerprints, token) and collaborates with the security card and a key-server LSS in authenticating the user. After authentication, the security card obtains, from a key-server LSS, the authorization information and/or group keys associated with the user, which allow it to perform object encryption/decryption on behalf of the user. If the LSS's initialization is performed in one phase, everything is done while a user is authenticated.

A.4.5 VPNs

VPNs can be implemented by supporting nodes and be based on firewalls/NEUs. Even though guards are not required, they can be used as LSS nodes in place of firewall/NEUs if the system is not connected to any CBIS systems, for instance.

A.4.6 Generic CBIS architecture: advantages and limitations

The Generic CBIS architecture has the following advantages and limitations:

Advantages:

A1) Physical protection. As noted in L9 below, the physical security of the two previous architectures must be reinforced because users of different information domains may be present in a LAN.

A2) Logical protection. Guards enforcing information domain security policies are not assumed here even if there exist inter-domain information exchange mechanisms. Hence, firewalls/NEUs can be used as boundary controllers for LANs.

A4) Automated inter-domain exchange mechanisms. It is assumed here that at least one LSS can perform the exchange operation. For instance, this LSS can be an MLS-user LSS or an MLS-guard LSS if domains support an MLS security policy.

A5) Confidentiality/integrity/strong authentication. The architecture provides

- Confidentiality/integrity protection of information while information is in transit within and outside LANs.
- Strong authentication mechanisms to prevent logical access to unauthorized users that have physical access to LANs.

A6) Multiple domain support for LANs. The Generic CBIS architecture compared to the two previous architectures minimizes the number of LANs necessary for a system.

Limitations: L1-L4 and L6 are no longer limitations.

L5) Security model problem.

L7) New mechanisms for information exchange are needed. Even though (L4) is not a limitation because firewall/NEUs can be used, if exchanges between information domains are needed, this exchange service needs to be done by one or more LSSs. It is not clear if it is easier to make such LSSs than to make a guard for the previous architecture. However, in a system with many LANs, it is possible that a single LSS node provides an exchange service for all the system.

L8) Cost of LSS nodes. LSS nodes are more expensive than end-systems. Moreover, different types of LSS systems need to be developed to achieve systems with desired functionalities, implying development costs.

L9) The problem of unauthorized information flows due to workstations. In the Generic CBIS architecture, a workstation may contain information from different information domains over a period of time; this risk is not present in the two other architectures. For instance, a member of a domain1 that is not a member of a domain2 may have physical access to domain2's residual information located on workstations. So, measures must be implemented to prevent/mitigate leakage of information on workstation between user sessions. Note that this problem may be present also for servers. However, servers may not be physically accessible to users.

L10) Cost of strong authentication mechanisms needed. Strong authentication mechanisms are needed because users can belong to different information domains and work in the same physical environment. In the two other architectures, strong authentication may be not required because all users of a LAN belong to the same information domain.

Table 1, following, summarizes the advantages and limitations of the three architectures.

Advantages\ Architectures	Traditional architecture/Single information domain	Multi information domain architecture	Generic CBIS architecture
A1) Physical protection	X	X	X
A2) Logical protection	X	X	X
A3) Security model based	X		
A4) Automated inter-domain exchange mechanisms		X	X
A5) Confidentiality/integrity/Strong authentication			X
A6) Multiple domain support for LANs			X
Limitations:			
L1) No automated inter-domain exchange mechanisms	X		
L2) High hardware and management costs	X		
L3) Confidentiality/Integrity/authentication weaknesses	X	X	
L4) Guard implementation problem		X	
L5) Security model problem		X	X
L6) Single information domain support for LANs	X	X	

L7) New mechanisms for information exchanges are needed			X
L8) Cost of LSS nodes			X
L9) The problem of unauthorized information flows due to workstations.			X
L10) Cost of strong authentication mechanisms needed			X

Table 1: Advantages and limitations of the three architectures

Appendix B: Presentation slides

Presentation 1: MLM: Coordinating Network Management Across Security Boundaries using Policy Resolution, David Kidston, CRC

Slide 1



Communications Research Centre
Canada
An Agency of Industry Canada

Centre de recherches sur les communications
Canada
Un organisme d'Industrie Canada

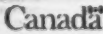


MULTI-LEVEL MANAGEMENT

Coordinating Network Management
Across Security Boundaries Using
Policy Resolution

David Kidston, crc

April 2005



Delivers R&D Canada - Ottawa



CENTRE de RECHERCHES COMMUNICATIONS
RESEARCH CENTRE

Slide 2

Overview

Background

- TTCP C3I commissioned a PA on coalition network management starting Dec 2000 and lasting three years. Demonstration Fall 2003.
- PA demonstrated the principles of autonomy, visibility, and coordination of network management within a coalition network.

Questions of interest today

- What is the difference between a security domain and a management domain?
- How much information must pass between security domains to co-ordinate coalition-wide network management
- How can policy be used to integrate cross-domain network services, including management



Slide 3

The Project Arrangement

CNMS Objectives

- Develop, implement and demonstrate a coalition network management system (CNMS).
- Bring together in-house NM research programs of DSTO (Australia), CRC (Canada) and AFRL (USA).
- Development Philosophy (NM focus): "share with partners yet retain control of your assets"
- Project emphasis:
 - Cross-domain management and issues related to National and Coalition enclaves
 - Operation in a bandwidth impoverished environment
 - Policy for implementing enterprise level objectives

*Confidentiality
Integrity
Availability*



Slide 4

Coalition Networks

Problem Area

- Lack of Coalition Information Systems Interoperability
- Specific to this project arrangement; inability to Manage the infrastructure of a coalition network connecting national networks



Slide 5

Research Areas

Canada

CRC Low BW Mgmt work

Australia

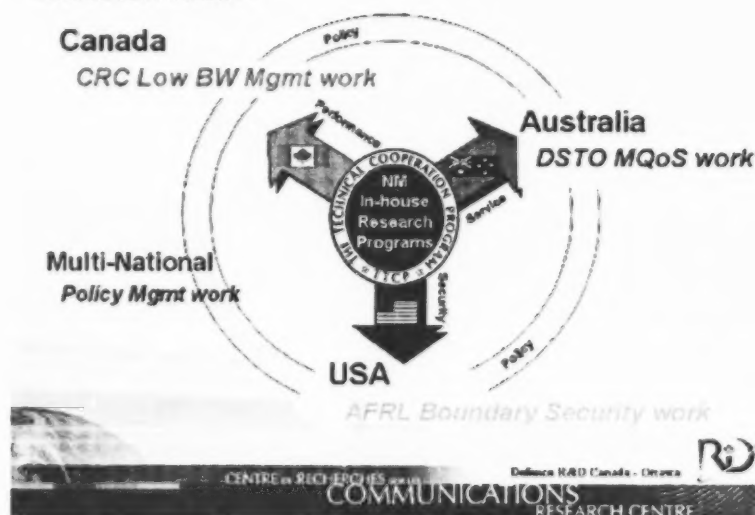
DSTO MQoS work

Multi-National

Policy Mgmt work

USA

AFRL Boundary Security work



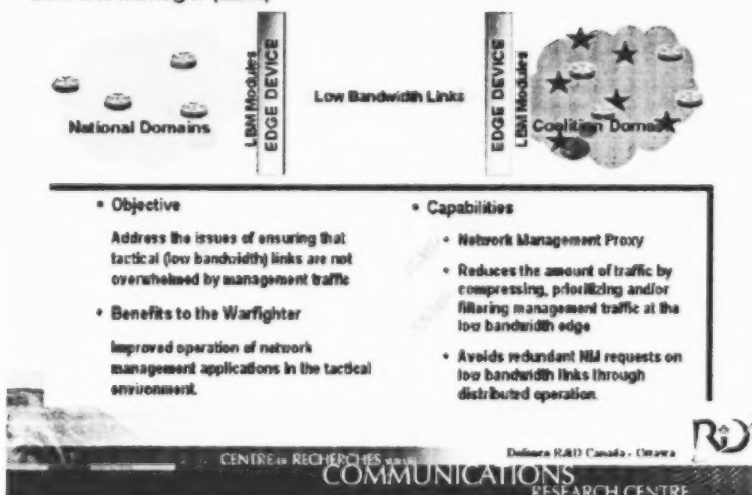
AUS RESEARCH

Military-Oriented QoS through Bandwidth Brokerage (BB)



CAN RESEARCH

Low BW Manager (LBM)



AUS RESEARCH

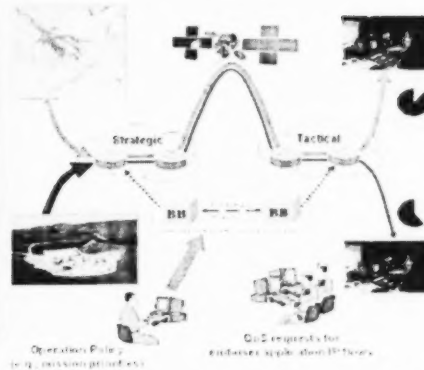
Military-Oriented QoS through Bandwidth Brokerage (BB)

AIM

Design, demonstrate and evaluate Bandwidth Broker approach to support Military QoS (M-QoS) for Australian Defence and Coalition IP networks

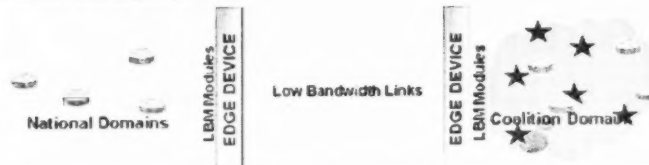
NEW CAPABILITIES

- Mission critical service assurance in heavily loaded, capacity constrained networks
- Automated admission control and dynamic prioritisation according to military importance
- Graceful degradation in QoS
- Imposed limitations for duration and demand of high priority flows



CAN RESEARCH

Low BW Manager (LBM)



• Objective

Address the issues of ensuring that tactical (low bandwidth) links are not overwhelmed by management traffic

• Benefits to the Warfighter

Improved operation of network management applications in the tactical environment

• Capabilities

- Network Management Proxy
- Reduces the amount of traffic by compressing, prioritizing and/or filtering management traffic at the low bandwidth edge
- Avoids redundant NIM requests on low bandwidth links through distributed operation





Policy-Based Network Management



Slide 10

Multi-National Contribution Policy Management

Collaboratively designed and developed

PDP-PEP communications framework (developed by AFRL)

- Each nation used the PDP-PEP framework to policy enable their individual network elements (BB, MCI, ACI, LBM)

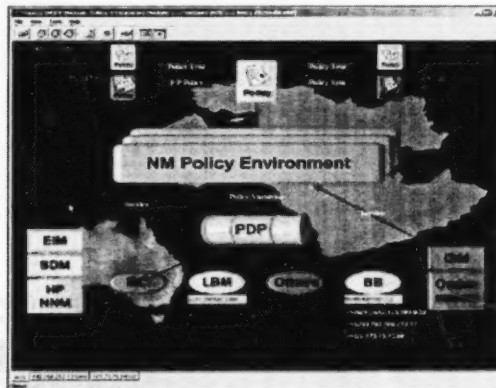
Domain Policy Integration Manager (DPIM) (developed by DSTO)

- Acts as the PBNM console for Enterprise Policy
- High Level XML policy representation
- Coordinates interactions with lower level system entities including event collection through PDP-PEP framework
- Communicates and coordinates with peer DPIMs (Both National DPIM AND other CHOC DPIMs)



Slide 11

Policy-Based Network Management Domain Policy Integration Manager (DPIM)



Slide 12

The Second CNMS Demonstration

Completed Dec 2003 between AFRL, DSTO & CRC

Focus: Integrated Symmetrical CNMS

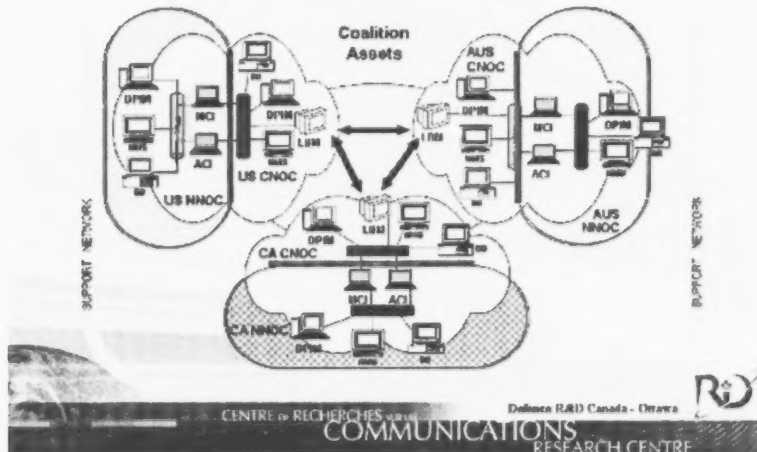
- High degree of NM technology **Capability**
- High degree of NM technology **Integration**
 - Management Controlled Interface, Application Controlled Interface, Bandwidth Broker, Low Bandwidth Manager, and DPIM
- Fully **Policy enabled** NM architecture



Slide 13

CNMS Demonstration 2

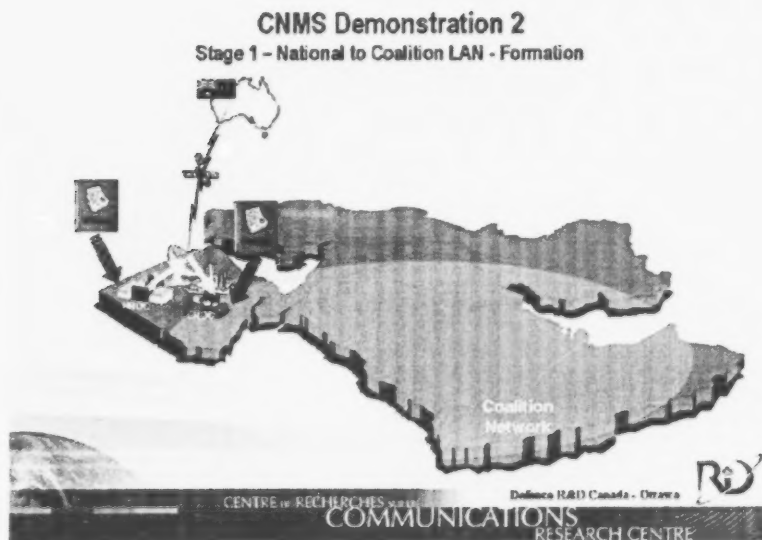
Symmetric Coalition Operation Center Architecture



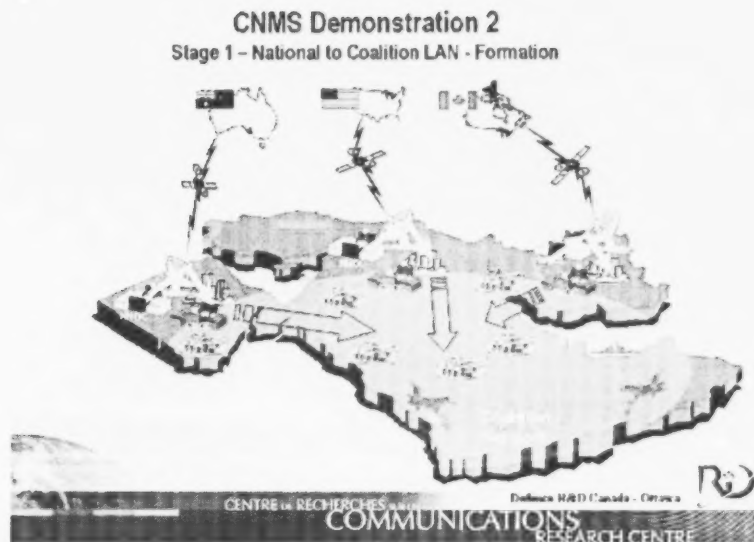
Slide 14



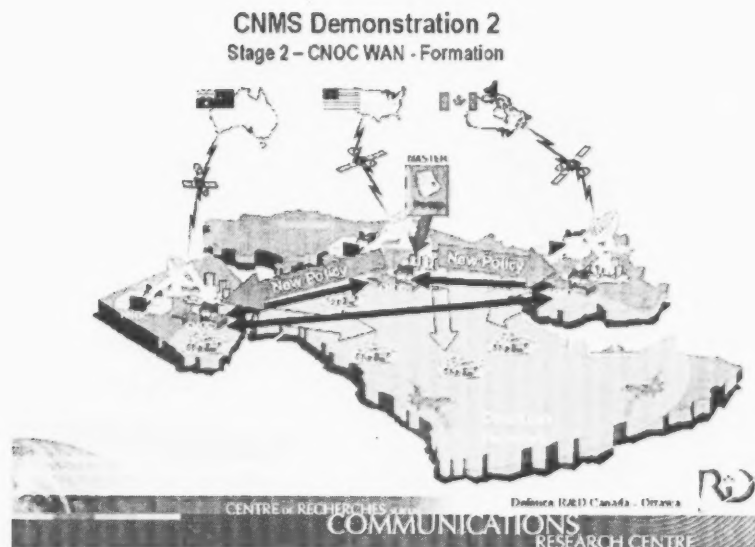
Slide 15



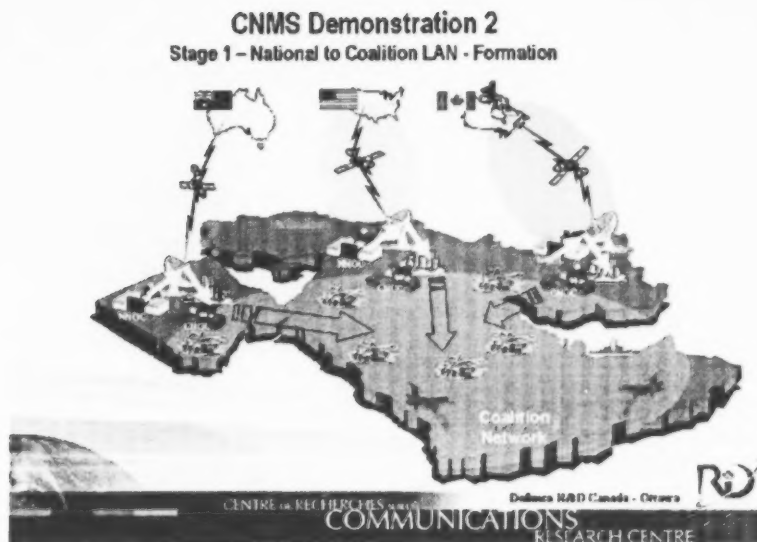
Slide 16



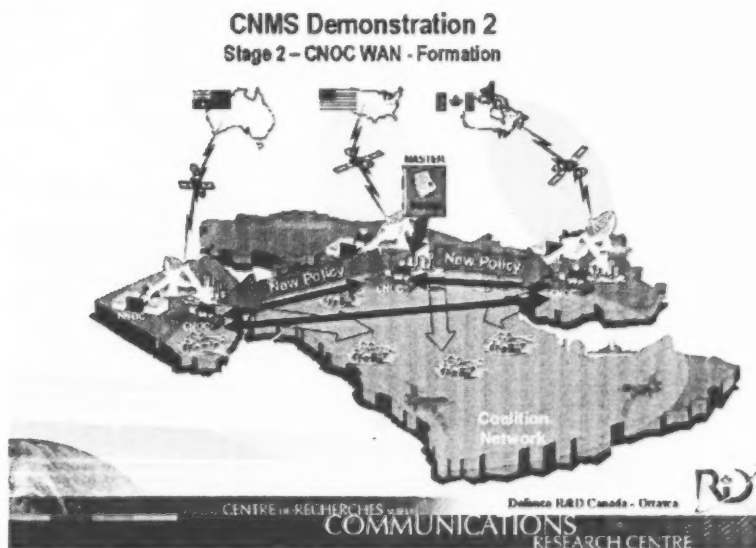
Slide 17



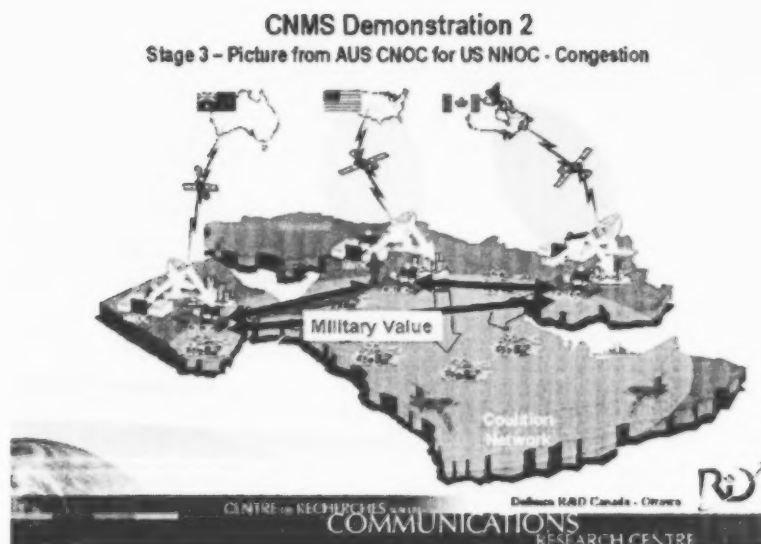
Slide 16



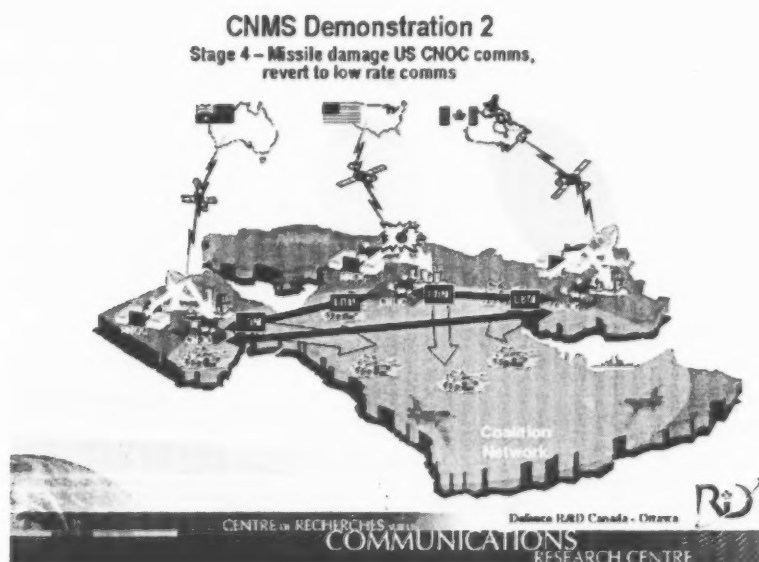
Slide 17



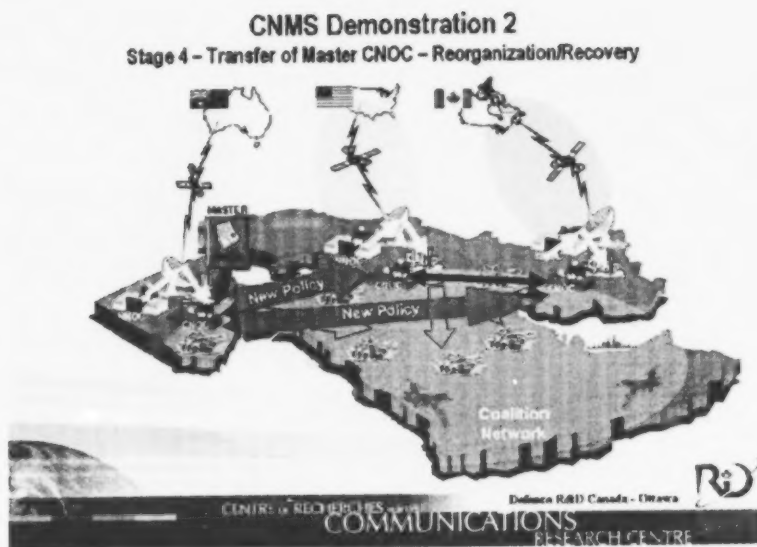
Slide 18



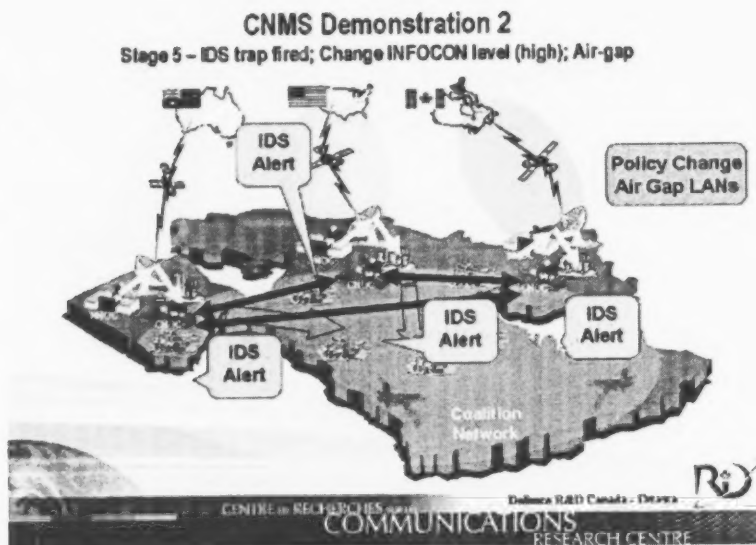
Slide 19



Slide 20



Slide 21



Slide 22

CAPABILITY SUMMARY

- Policy Enabled Enterprise Management – Rapid response to multiple INFOCON/ALERT Levels
- Management Controlled Interface AND Application Controlled Interface for cross domain traffic
- Low Bandwidth Management to reduce network traffic on disadvantaged links
- Military Quality of Service Components using Bandwidth Broker
- CNMS Infrastructure: Voice Over IP, IPSec tunnels, ISDN, Symmetrical Architecture (enables any CNOC to be in control of the mission), VTC via IPSec tunnels over internet, standard DNS, email services, chat, ftp etc...

Coordination of collective behaviour in response to changing enterprise requirements

Network C2P & Security

Mission Critical Flows

Trunk Efficiency

Autonomous
Visibility
Coordination

CENTRE DE RECHERCHES COMMUNICATIONS
RESEARCH CENTRE

Defence R&D Canada - Ottawa



Slide 23

Conclusions: CNMS and Multi-Level Security

How can policy be used to integrate cross-domain network services, including management?

- This was the focus of the PA.

How much information must pass between security domains to co-ordinate coalition-wide network management?

- Policy at a minimum. Further information may be permitted based on the visibility desired and international cooperation (resolved policy).

What is the difference between a security domain and a management domain?

- This is really the purview of multi-level security. Though it was not addressed directly in this work, it would be a valuable (and necessary) contribution to a future deployed system.

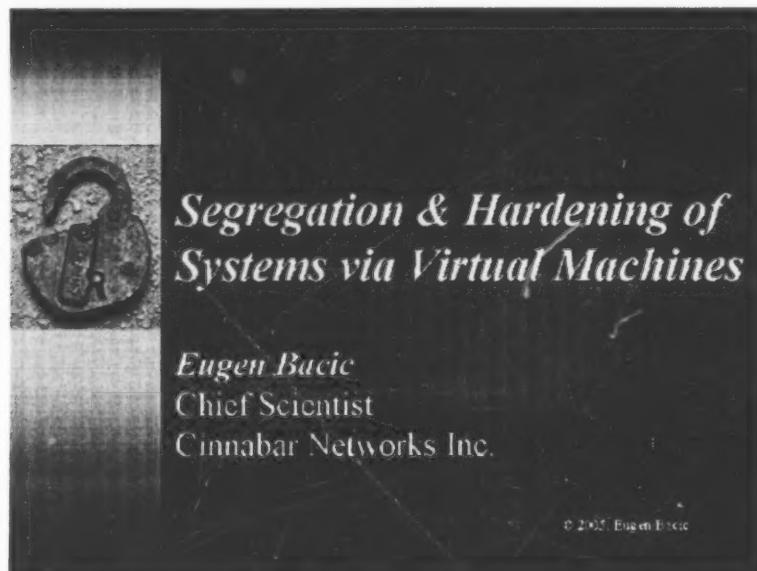
CENTRE DE RECHERCHES COMMUNICATIONS
RESEARCH CENTRE

Defence R&D Canada - Ottawa

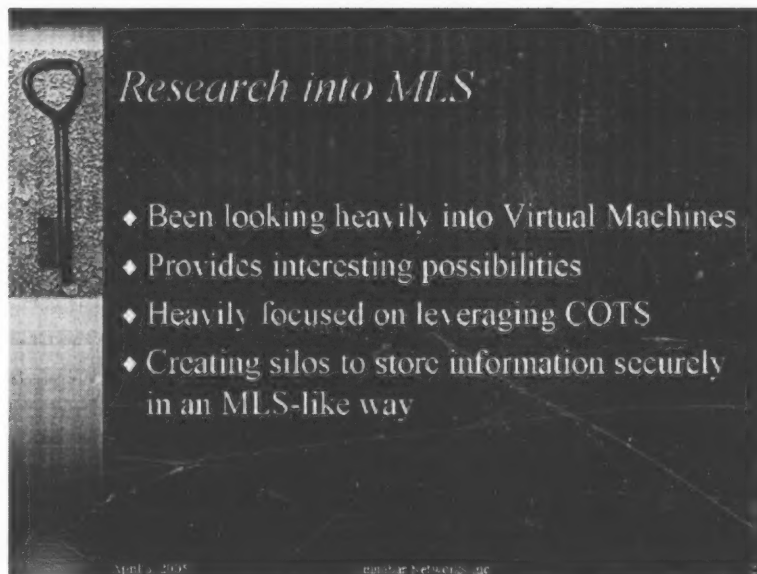


Presentation 2: Segregation & Hardening of Systems via Virtual Machines, Eugene Bacic, Cinnabar Networks Inc.

Slide 1



Slide 2



Slide 3

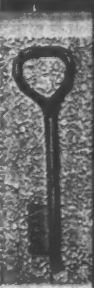


Virtual Machines

- ◆ Provide ability to run multiple, separate machines
- ◆ Each has its own memory and disk storage as well as virtualized network devices, etc.
- ◆ Host OS acts as virtualized hardware layer
- ◆ Lots of potential

April 2, 2005 Senior Network Eng

Slide 4



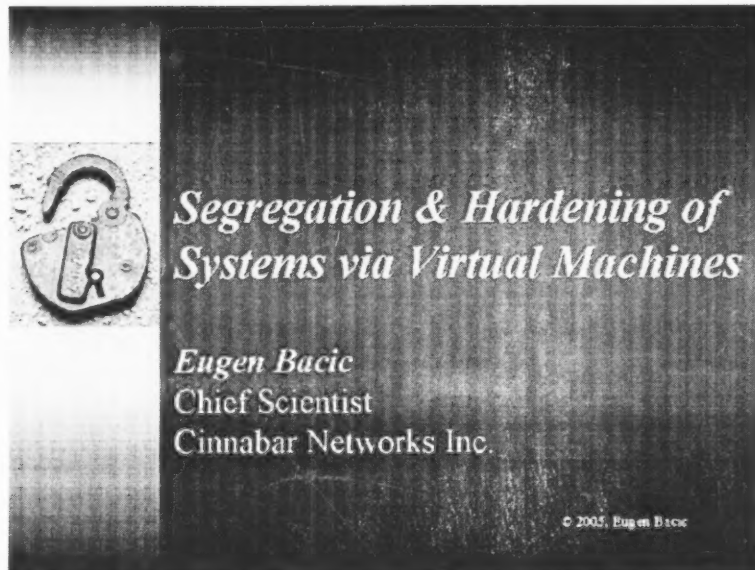
Host OS as HAL

- ◆ Host OS is effectively hardware that is:
 - Easily modifiable
 - Programmable
 - Malleable
- ◆ Even more so if you use *Linux*

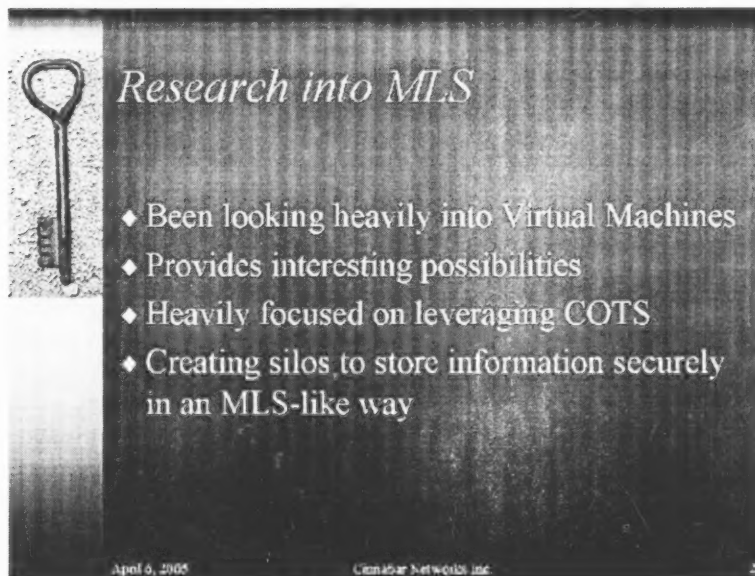
April 2, 2005 Senior Network Eng

Presentation 2: Segregation & Hardening of Systems via Virtual Machines, Eugene Bacic, Cinnabar Networks Inc.

Slide 1



Slide 2



Slide 3



Virtual Machines

- ◆ Provide ability to run multiple, separate machines
- ◆ Each has its own memory and disk storage as well as virtualized network devices, etc.
- ◆ Host OS acts as virtualized hardware layer
- ◆ Lots of potential

April 6, 2005 Citicorp Networks Inc. 3

Slide 4

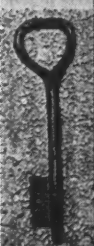


Host OS as HAL

- ◆ Host OS is effectively hardware that is:
 - Easily modifiable
 - Programmable
 - Malleable
- ◆ Even more so if you use *Linux*

April 6, 2005 Citicorp Networks Inc. 4

Slide 5

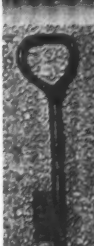


Flavours of Silos

- ♦ VM Guest OS can be viewed as silos
- ♦ Goal is to harden and define a silo to a specific classification
- ♦ Allows for interesting possibilities
 - Use of encrypted Guest OS images
 - Use of external devices: thumb drives, etc.
 - Centralized image activation
 - LDAP, Policies, Audit, ...
- ♦ Not 100% MLS, but getting closer

April 1, 2005 www.northern.ca

Slide 6

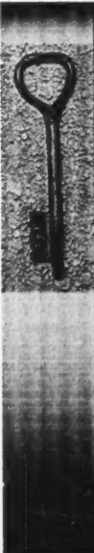


Advantages

- ♦ Simpler access to unified cryptography
- ♦ Uniform hardening techniques
- ♦ Centralized control of VMs
- ♦ Possibility of policy-driven operation
- ♦ Centralized, intelligent monitoring via coherent/consistent audit

April 1, 2005 www.northern.ca

Slide 7



Disadvantages

- ♦ Still suffers from *cut & paste* issues
- ♦ Not a "single desktop" paradigm
- ♦ Learning curve
- ♦ Unknown security issues

April 3, 2005 © Citigroup Networks Inc.

Slide 8



Partial Solutions

- ♦ USB thumb drives
- ♦ Restricted VM images
- ♦ Virtualized sessions via the Web

April 3, 2005 © Citigroup Networks Inc.

Slide 5



Flavours of Silos

- ♦ VM Guest OS can be viewed as silos
- ♦ Goal is to harden and define a silo to a specific classification
- ♦ Allows for interesting possibilities
 - Use of encrypted Guest OS images
 - Use of external devices: thumb drives, etc.
 - Centralized image activation
 - LDAP, Policies, Audit, ...
- ♦ Not 100% MLS, but getting closer

April 6, 2005 Canabur Networks Inc. 5

Slide 6



Advantages

- ♦ Simpler access to unified cryptography
- ♦ Uniform hardening techniques
- ♦ Centralized control of VMs
- ♦ Possibility of policy-driven operation
- ♦ Centralized, intelligent monitoring via coherent/consistent audit

April 6, 2005 Canabur Networks Inc. 6

Slide 7



Disadvantages

- ◆ Still suffers from *cut & paste* issues
- ◆ Not a “single desktop” paradigm
- ◆ Learning curve
- ◆ Unknown security issues

April 6, 2005 Citinabar Networks Inc.

Slide 8



Partial Solutions

- ◆ USB thumb drives
- ◆ Restricted VM images
- ◆ Virtualized sessions via the Web

April 6, 2005 Citinabar Networks Inc.

Slide 9



MLS iPods

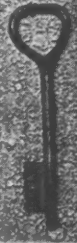


- ◆ Each iPod holds MLS data
- ◆ Data is encrypted
- ◆ Access is granted by Host OS
- ◆ Host OS duplicates data into RAM
- ◆ Slow, but possible
- ◆ Interesting direction

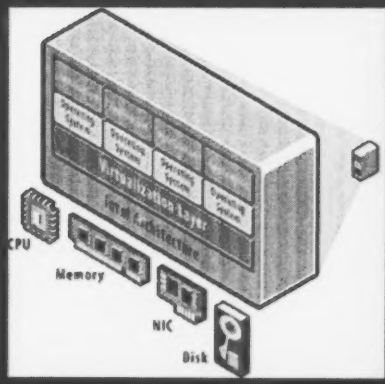
From iPodPAID: www.scribble.org.com/articles/00015.html

April 2005 Canadian Networks Inc.

Slide 10

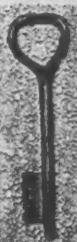


Restricted VM Images



- ◆ Each VM operates in own domain, creating a silo
- ◆ Shares CPU, Memory, network, etc.
- ◆ Does not solve all problems

April 2005 Canadian Networks Inc.



Web-based Virtualization

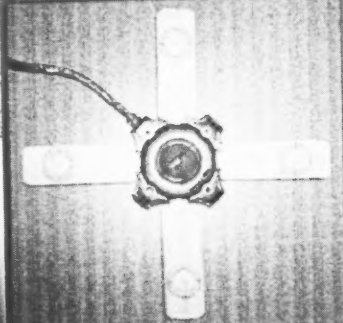
- ◆ Other areas that are interesting:
 - AppGate
 - Citrix Metaframe
 - Terminal Services in general
- ◆ Use of browsers allows for:
 - Simple desktop OS / Thin client
 - Elimination of local storage concerns
 - No need for “special” hardware solutions
- ◆ However, no OS currently available

APRIL 9, 2005 Microsoft Network Ltd. 11

Slide 9



MLS iPods



- ◆ Each iPod holds MLS data
- ◆ Data is encrypted
- ◆ Access is granted by Host OS
- ◆ Host OS duplicates data into RAM
- ◆ Slow, but possible
- ◆ Interesting direction

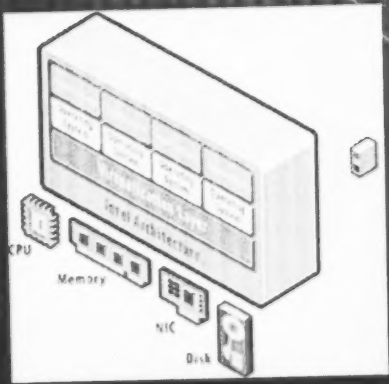
From iPod P.A.M. at www.wiredthisway.com/Articles/000154.html

April 6, 2005 Cinnabar Networks Inc.

Slide 10



Restricted VM Images



- ◆ Each VM operates in own domain, creating a silo
- ◆ Shares CPU, Memory, network, etc.
- ◆ Does not solve all problems

April 6, 2005 Cinnabar Networks Inc.



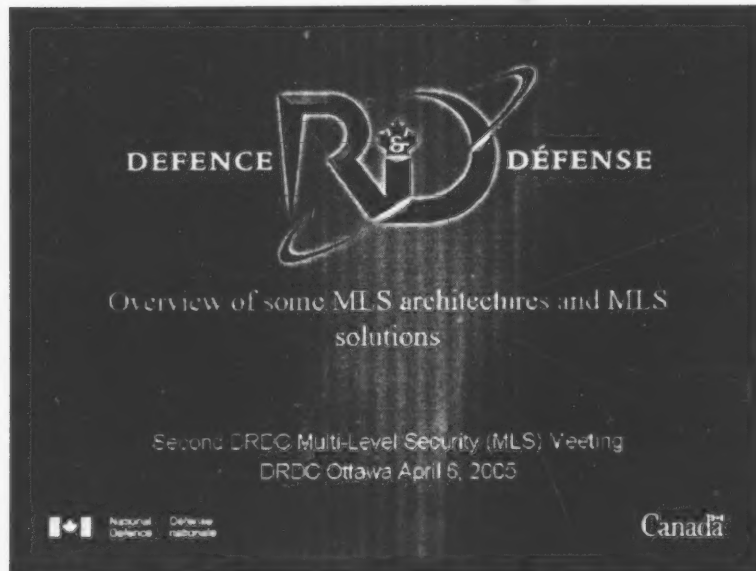
Web-based Virtualization

- ◆ Other areas that are interesting:
 - AppGate
 - Citrix Metaframe
 - Terminal Services in general
- ◆ Use of browsers allows for:
 - Simple desktop OS / Thin client
 - Elimination of local storage concerns
 - No need for "special" hardware solutions
- ◆ However, no OS currently available

April 6, 2005 Citrix Networks Inc. 11

Presentation 3: Overview of some MLS architectures and MLS solutions, Jean Savoie, NIO Section, DRDC Ottawa

Slide 1



Slide 2



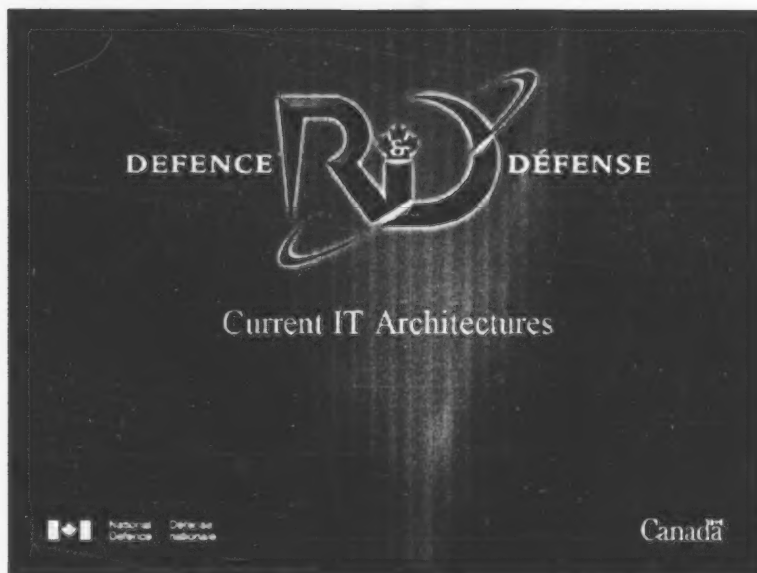
Agenda

- Current IT architectures
 - Many networks
 - System-High Enclave (SHE)
 - Linked SHEs
- Content Based Information Security (CBIS)
 - A single network
- Global Information Grid (GIG) (if time allows it)



DRDC Ottawa

Slide 3



Slide 4

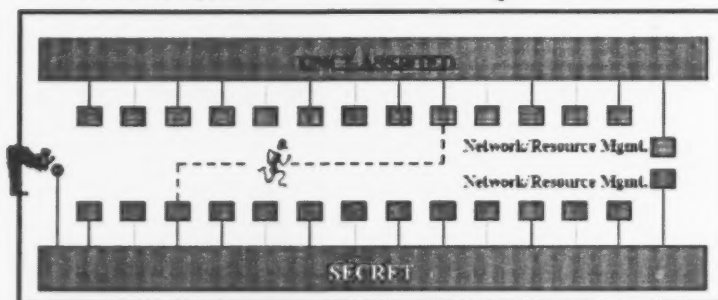
System-High Enclave (SHE) Architecture

All users are cleared to access all information

Physical security provided by the enclave boundary

Can contain a single network

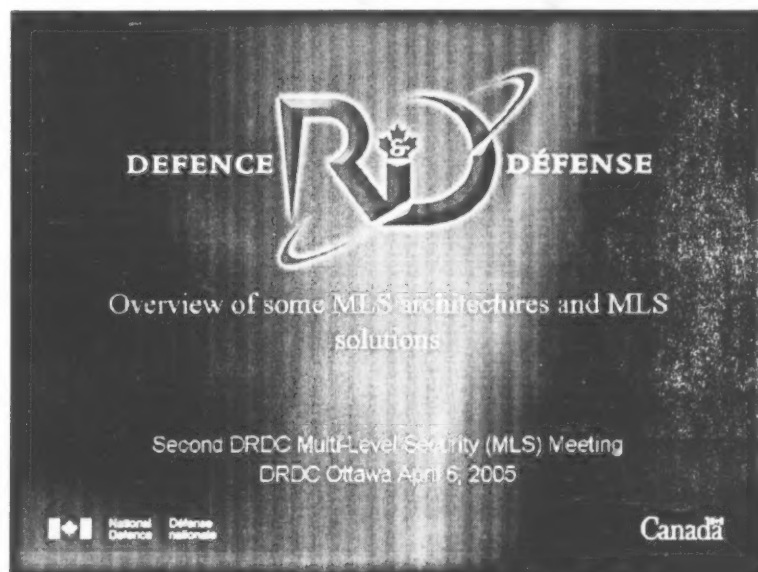
Secret SHE



- No electronic labeling of information assumed
- Information separation through separated networks
- Information flows between networks are often through air-gaps

Presentation 3: Overview of some MLS architectures and MLS solutions, Jean Savoie, NIO Section, DRDC Ottawa

Slide 1

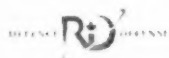


Slide 2



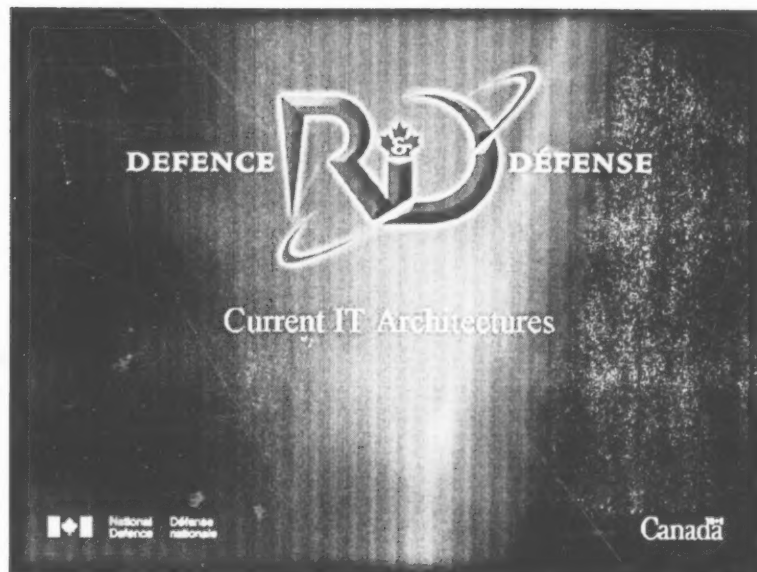
Agenda

- Current IT architectures
 - Many networks
 - System-I high Enclave (SHE)
 - Linked SHEs
- Content Based Information Security (CBIS)
 - A single network
- Global Information Grid (GIG) (if time allows it)



DRDC Ottawa

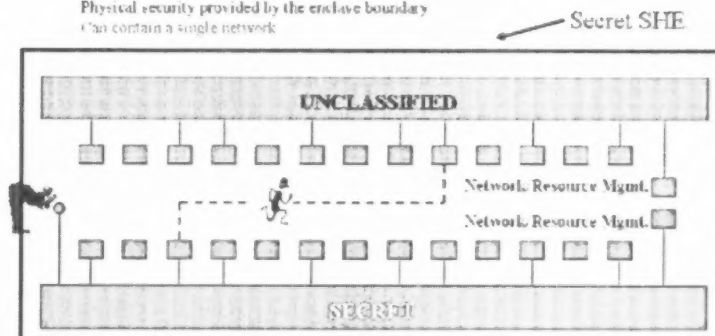
Slide 3



Slide 4

System-High Enclave (SHE) Architecture

All users are cleared to access all information
Physical security provided by the enclave boundary
Can contain a single network



- No electronic labeling of information assumed
- Information separation through separated networks
- Information flows between networks are often through air-gaps



SHE Architecture: Advantages

- **Due to the physical environment**
 - Standard physical security measures are known
 - Red networks (in the enclave) can be acceptable
 - Authentication mechanisms can be less robust from inside the enclave
- **No electronic labeling necessary**
- **Low number of IT security services needed**
 - Manual flow controls



DRDC Ottawa



SHEs satisfy Bell-Lapadula model

- Information is implicitly labeled by networks
- Information flows from High to Low are allowed only through trusted processes (users)



DRDC Ottawa



SHE Architecture: Problems

- Applications cannot cross security boundaries; no efficient information sharing
- Procedural flow controls between networks (no automation and labor intensive)
- Need separate Network/Resource Mgmt for each Level
- Duplication of workstations/servers/services
So, expensive in management and resources and provide few automated services. Inhibit business processes .So, more services and more resource sharing are needed.



DRDC Ottawa



Linked SHEs

- Connection architecture
 - Connection between networks of different classifications
 - Guards and specialized systems
 - Connection between network of same classification
 - VPNs/ NEUs + other technology?
- Service architecture
 - Mail, directory, DNS services
 - Web services (push and pull)
 - Automated declassification/releasing
 - Flow of management data(IDS ?, IPSEC ?, SNMP?) and information



DRDC Ottawa

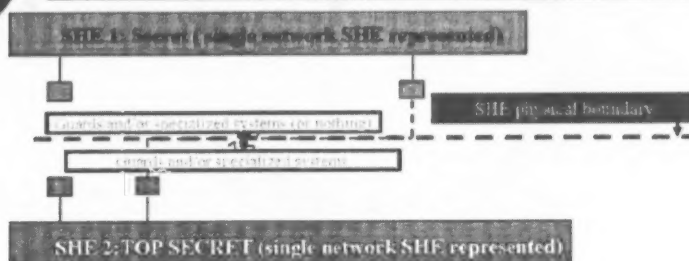
Slide 9

Linked SHEs: Connection Architecture I

Connection between networks of different classifications

Data flows controlled by guards and/or specialized systems

- Physical security



Generally: (1) Low-to-High data flows are filtered against malicious software
(2) High-to-Low data flows are content filtered and limited. Many applications are not allowed to cross SHE boundary.

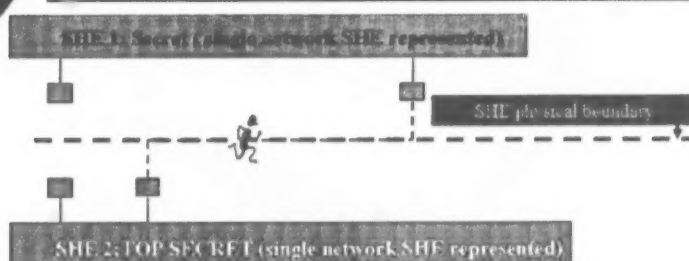


DRDC Ottawa

Slide 10

Linked SHEs: Connection Architecture I

Example I: Simple case



No automated flow transfers between networks

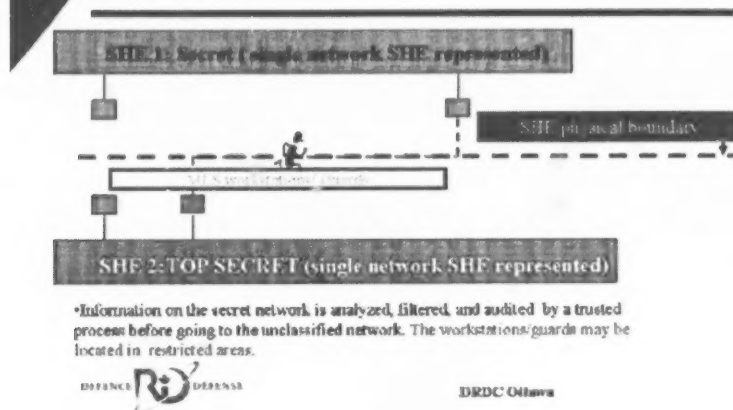


DRDC Ottawa

Slide 11

Linked SHEs: Connection Architecture I

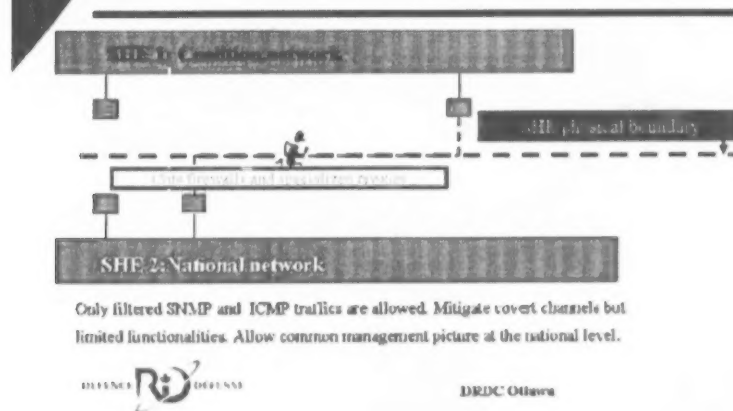
Example II: Flow controls through MLS workstations or guards



Slide 12

Linked SHEs: Connection Architecture I

Example III: Multi-Domain Network Management System
(See Managing Heterogeneous Networks Across Security/Coalition Domains of Scott Shyne and al)

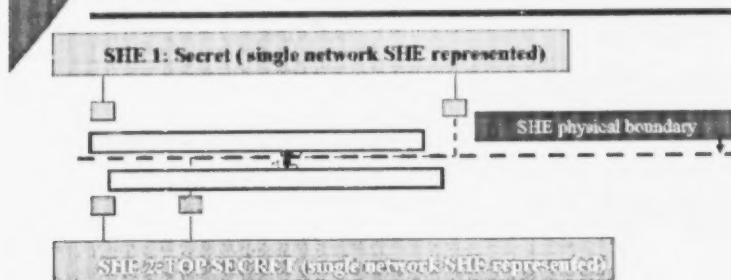


Slide 9

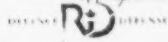
Linked SHEs: Connection Architecture I

Connection between networks of different classifications

Data flows controlled by guards and/or specialized system
- Physical security



Generally: (1) Low-to-High data flows are filtered against malicious software
(2) High-to-Low data flows are content filtered and limited. Many applications are not allowed to cross SHE boundary

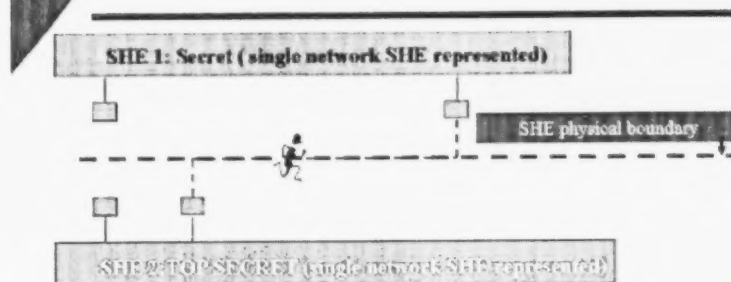


DRDC Ottawa

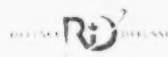
Slide 10

Linked SHEs: Connection Architecture I

Example I: Simple case



No automated flow transfers between networks

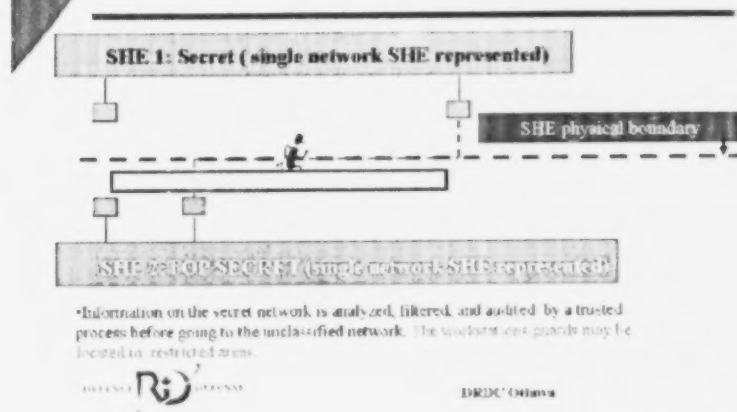


DRDC Ottawa

Slide 11

Linked SHEs: Connection Architecture I

Example II: Flow controls through MLS workstations or guards

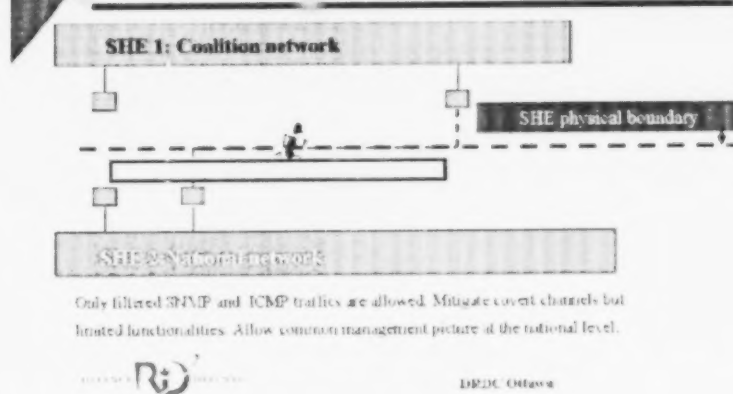


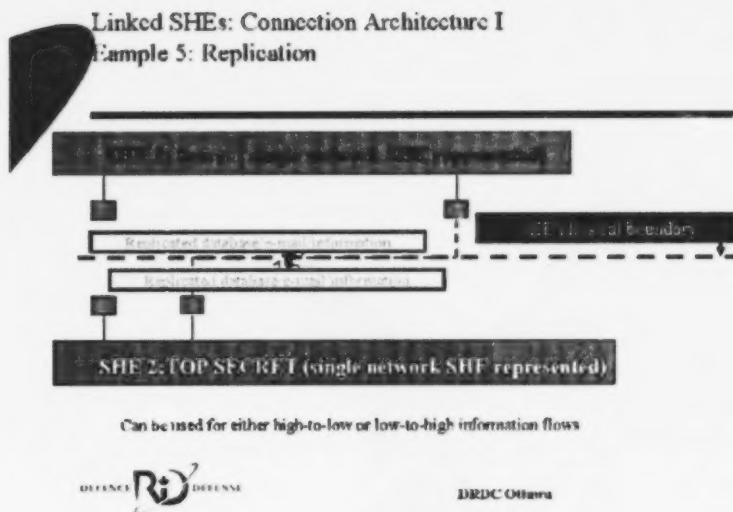
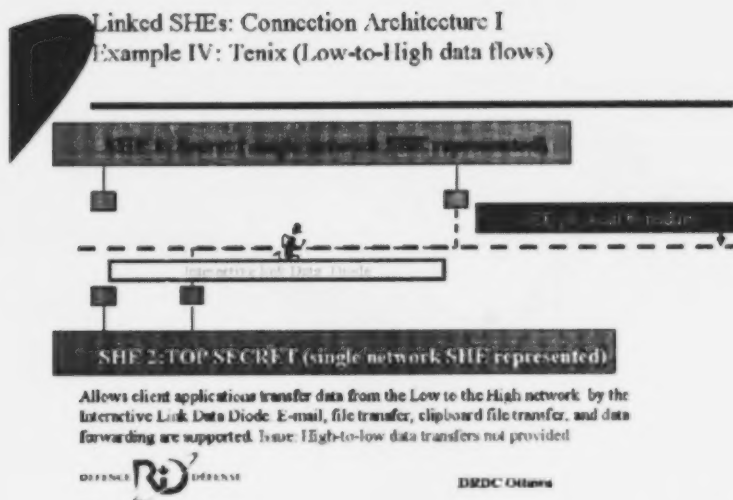
Slide 12

Linked SHEs: Connection Architecture I

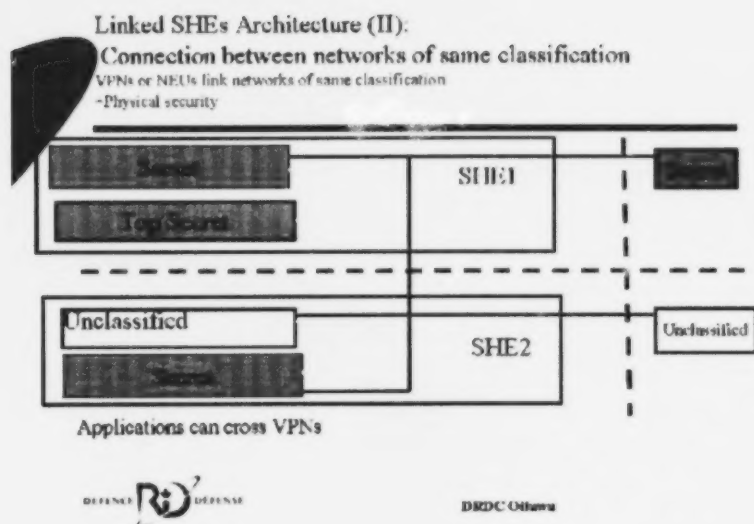
Example III: Multi-Domain Network Management System

(See: Managing Heterogeneous Networks Across Security/Coalition Domains of Scott Shyne and al)

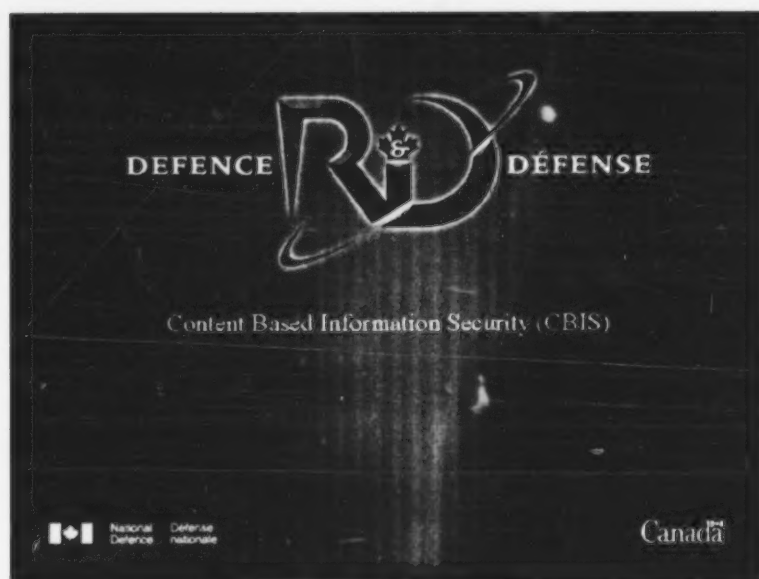




Slide 15

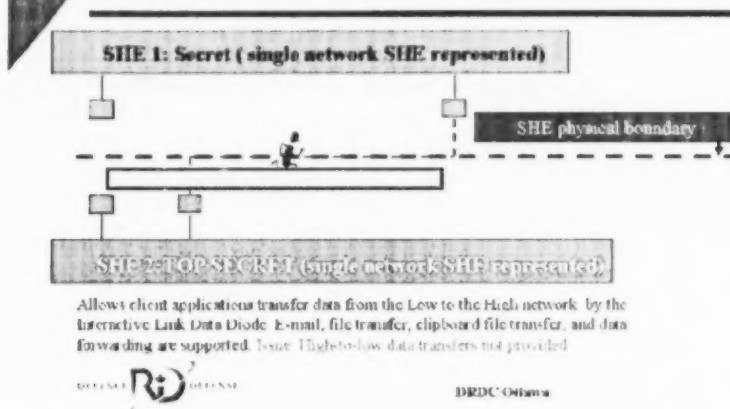


Slide 16



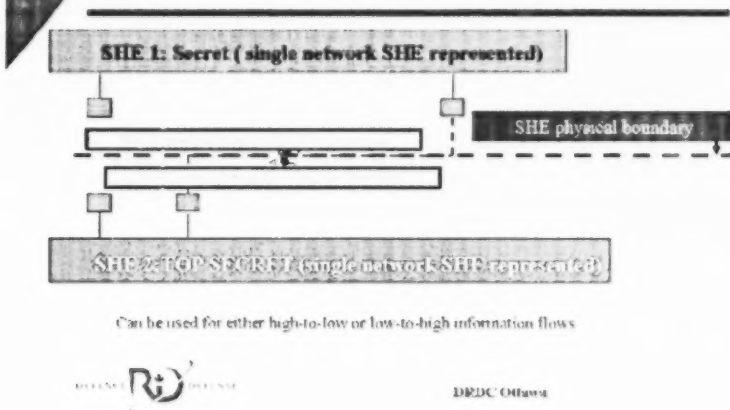
Slide 13

Linked SHEs: Connection Architecture I
Example IV: Tenix (Low-to-High data flows)

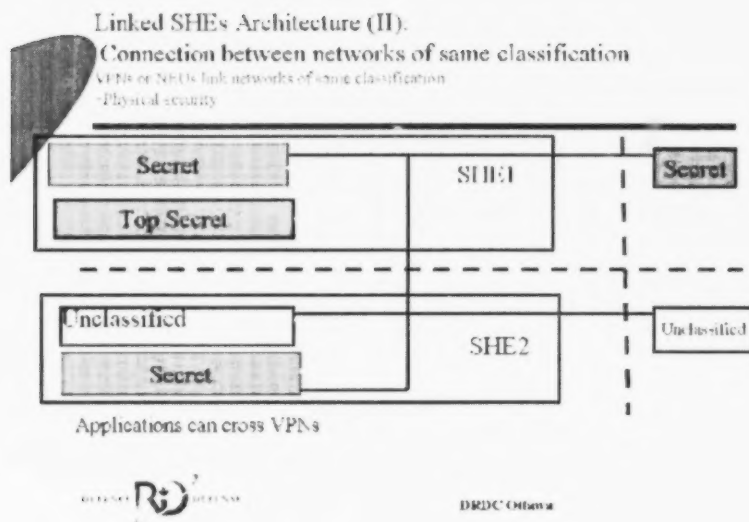


Slide 14

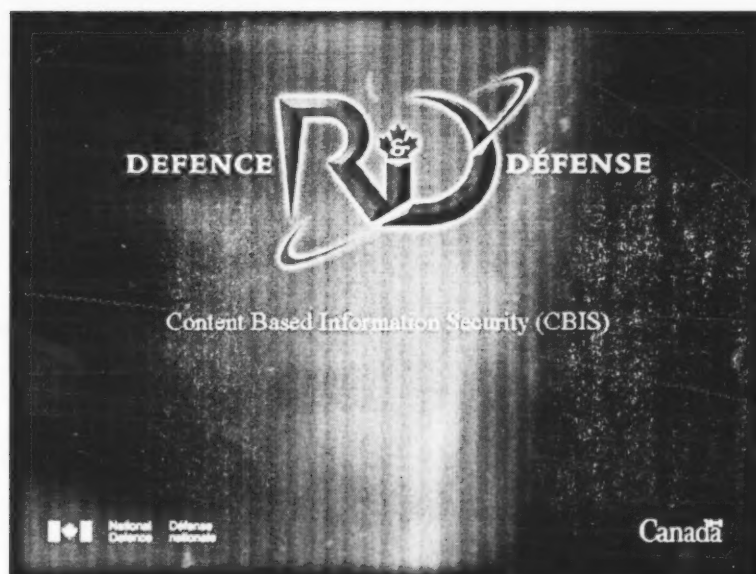
Linked SHEs: Connection Architecture I
Example 5: Replication



Slide 15



Slide 16

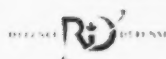


Slide 17



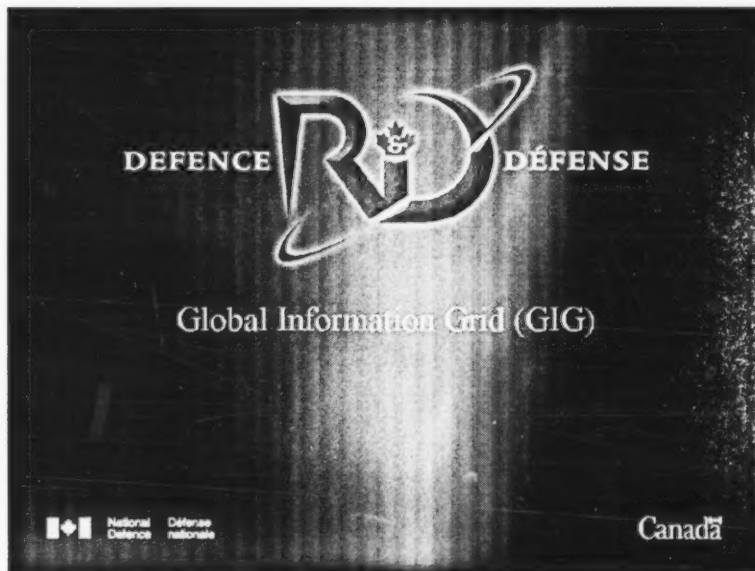
CBIS concepts

- A single network for information of all classifications and security domains
 - So the SHIE's networks are merged and information need to be separated
- Security domains are separated by
 - Encryption for information outside specialized nodes (e.g. desktops and guards)
 - Hardening the specialized nodes (e.g. workstation security improved by special security devices add-on to mitigate the risk inside these nodes)
- Physical security
 - TBD (for availability and integrity of information) Secret credential management procedures



DRDC Ottawa

Slide 18



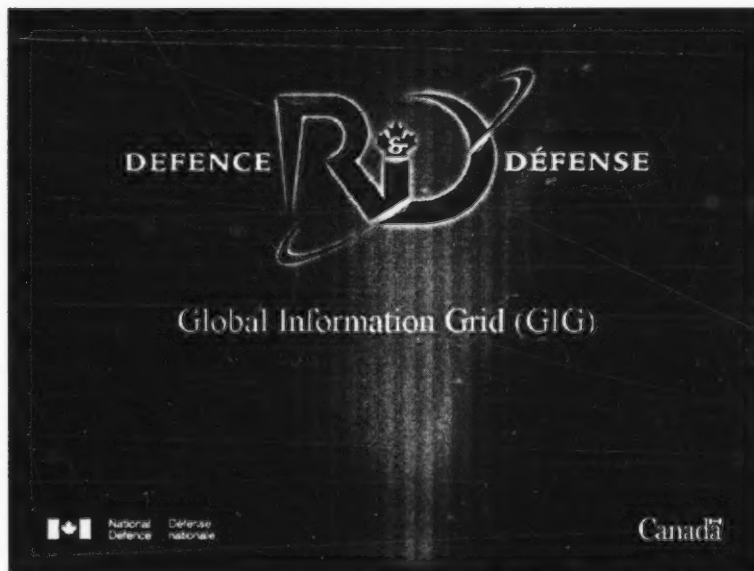


CBIS concepts

- A single network for information of all classifications and security domains
 - So the SHIE's networks are merged and information need to be separated
- Security domains are separated by
 - Encryption for information outside specialized nodes (e.g. desktops and guards)
 - Hardening the specialized nodes (e.g. workstation security improved by special security devices add-on to mitigate the risk inside these nodes).
- Physical security
 - TBD (for availability and integrity of information) Secret credential management + procedures



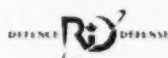
DRDC Ottawa





GIG Definition

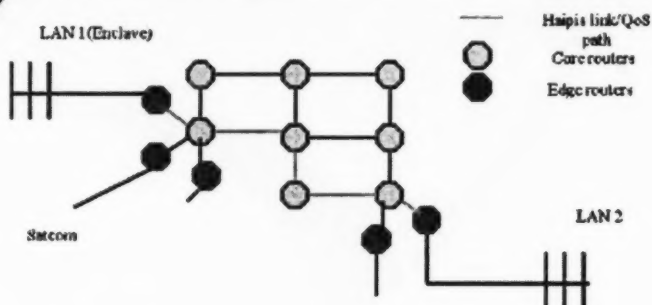
- Internet-like network but
 - Under a single administrative authority
 - The backbone provides new functions
- Provide many global services
 - Security services (e.g. authentication /authorization)
 - Functionality services (e.g. routing, QoS (need wide bandwidth), shared Web-server, knowledge databases, discovery)
 - Using these services it is assumed that it will be possible to build interoperable security domains.



DRDC Ottawa



GIG Bandwidth Expansion (GIG-BE)

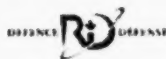


DRDC Ottawa



Security Services (II)

- Encryption
 - It would be useful to get such global services because it would be unnecessary to build a new encryption system for each new information domain (decrease the crypto management and provide a more uniform assurance).
- PKI and PMI
- Secure storage on servers?

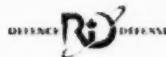


DRDC Ottawa



Security Services (II)

- Encryption
 - It would be useful to get such global services because it would be unnecessary to build a new encryption system for each new information domain (decrease the crypto management and provide a more uniform assurance).
- PKI and PMI
- Secure storage on servers?



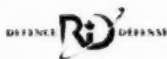
DRDC Ottawa

Slide 23



Security Services (III)

- Automated downgrading and releasing
 - Need labeling of information
- IDS
- Central and or local audit



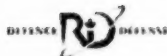
DRDC Ottawa

Slide 24



Functionality Services

- Secure routing
- Quality of Services (QoS)
- Push and Pull of information (Web-Server?)
- Knowledge management?
 - Discovery of information
 - Labeling
 - Storage of information

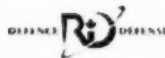


DRDC Ottawa



Building Security Domains

- It is assumed that it will be possible to build interoperable security domains.
- An security domain can be completely or partially logical.
 - i. Currently they correspond to physical networks. CBIS concepts can be used to implement them logically.
 - ii. Physical security should be very important too; especially for high classified domains



DRDC Ottawa



Building Information Domain (II)

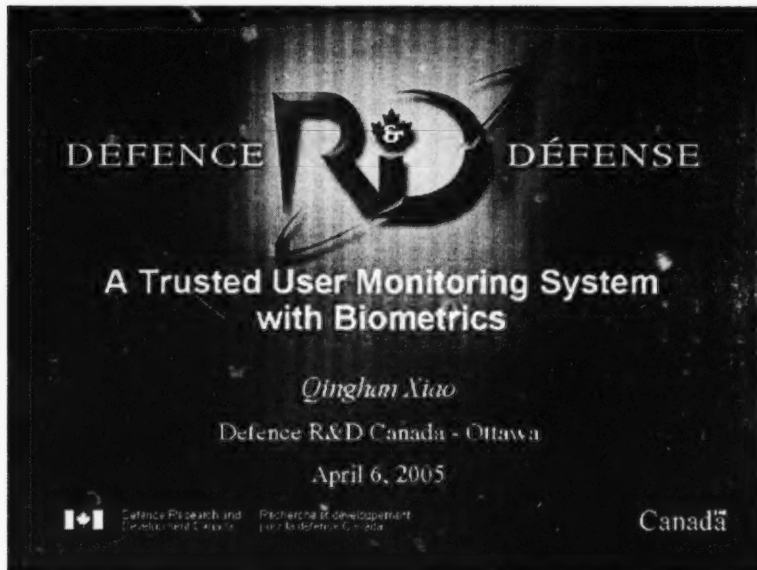
- It would be useful to get security domain profiles providing out-of-the-box solutions
 - Set the physical security
 - Standards for security policies
 - Set the mechanisms and services required



DRDC Ottawa

Presentation 4: A trusted user monitoring system with biometrics, Qinghan Xiao, NIO Section, DRDC Ottawa

Slide 1



Slide 2



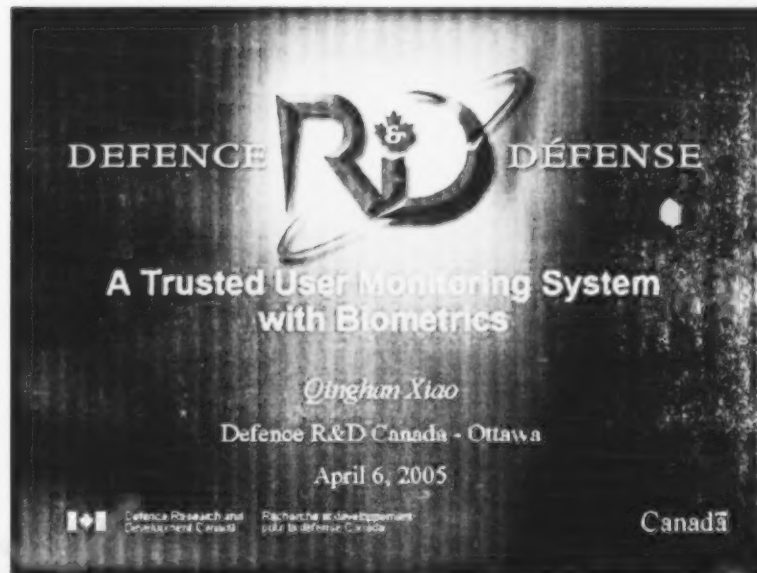
Outline

- Authentication
 - Locally (often controlled environment)
 - Remotely (may be open network)
- Biometric Authentication
 - Identity check
- Biometric Monitoring
 - Identity monitoring
- System Demonstration
 - Automatically log off a user when his/her face disappears from captured image frame for an adjustable time interval.

Defence R&D Canada - Ottawa • R & D pour la Défense Canada - Ottawa

Presentation 4: A trusted user monitoring system with biometrics, Qinghan Xiao, NIO Section, DRDC Ottawa

Slide 1



Slide 2



Outline

- Authentication
 - Locally (often controlled environment)
 - Remotely (may be open network)
- Biometric Authentication
 - Identity check
- Biometric Monitoring
 - Identity monitoring
- System Demonstration
 - Automatically log off a user when his/her face disappears from captured image frame for an adjustable time interval.

Slide 3



Authentication

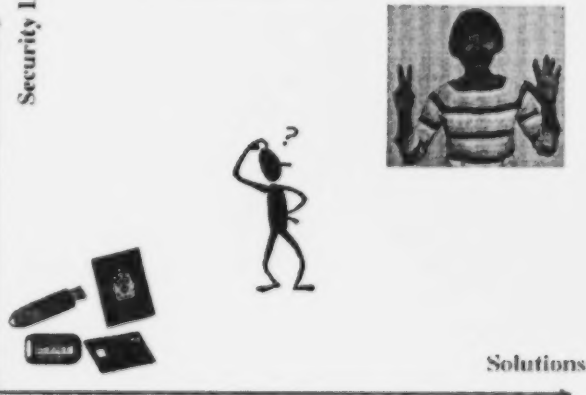
- Authentication is the first and most critical link in the security chain.
- It lets the authorized users access the system and data resource.
- Authentication can be divided into four categories
 - Local supervised
 - Local unsupervised
 - Remote supervised
 - Remote unsupervised

Defence R&D Canada - Ottawa • R & D pour la défense Canada - Ottawa

Slide 4

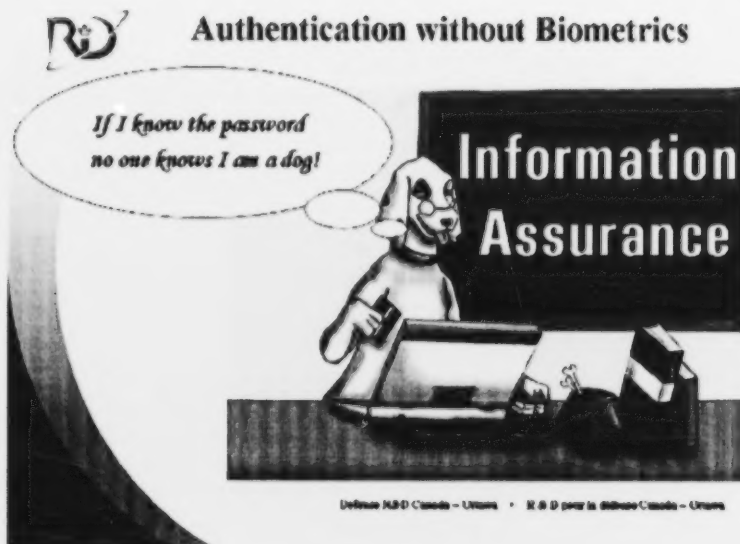


Authentication Factors

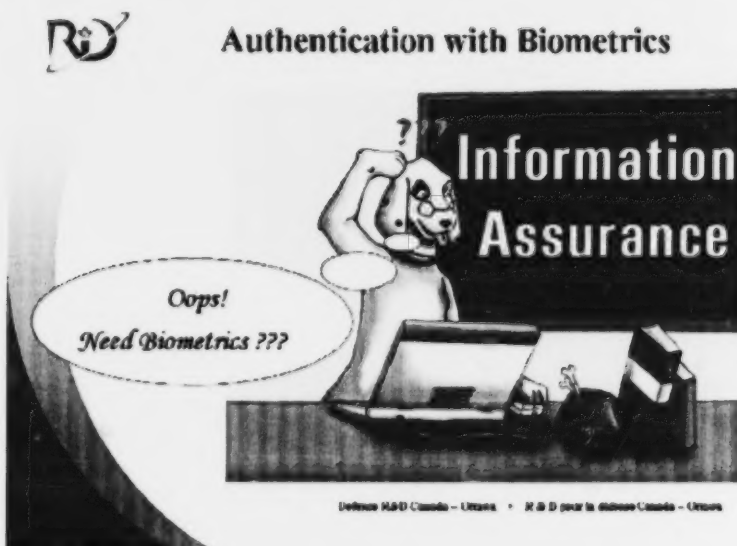


Defence R&D Canada - Ottawa • R & D pour la défense Canada - Ottawa

Slide 5



Slide 6





User Monitoring

- The identity of the user is checked by capturing the facial images at a certain time interval.
- If the user disappears or changes to someone else, the system will log off automatically.
- Not only does the system authenticate the user who originally logged onto the system, but also monitors the user who is conducting the communications.
- By incorporating multiple usages of biometrics, a higher degree of security can be achieved.

Defence R&D Canada - Ottawa • R & D pour la défense Canada - Ottawa

Appendix C: Questions asked to stakeholders

What is the single problem to be addressed by an MLS solution in the immediate term?

- User interface
- Policy and procedures for the use of MLS
 - Definition of a standard policy language/system or at least a direction for such
- What approaches to multi-caveat/multi-level separation will be certifiable
- Labelling and authorization
- To allow multiple domains of the same security classification to be accessed through the same workstation
- Encapsulation of information to provide simple, immediate tagging of information to assist in the creation of MLS solutions and labels
- Any MLS solution, whether it uses labels or other means to segregate data, must be simple and small enough to be evaluable (e.g., CC EAL4 and above, etc.).
 - Define "small". Many EAL4+ systems are anything but "small", although it's an excellent ideal
 - Interoperability between COTS solutions
- Which in turn will make solutions cheaper
 - While not increasing risk
- One desktop with multiple security domains
 - While not increasing risk
 - That can have some (limited) data sharing (e.g., read-down and write-up).
- Development of a departmental standard workstation configuration (hardware, software and operating system(s)) which could support implementation of processing multiple security levels on a single workstation platform, either through the use of virtual machine technology or something similar
 - Or be used across the Government of Canada
- Accreditation criteria and security policies to allow for MLS need to be reviewed in the light of the need to share information across domains. Most of the difficulties regarding MLS are cultural and organizational rather than technical.
- When to schedule the next MLS meeting?
- Is there a formal working group across the government?
 - We hope to have one within 12 months.
 - At the high level enterprise security architecture, at a more concrete level we need to addressing information labelling
- Start defining some business processes that we would like to protect and automate. This will help designing systems and procedures.
- Timeline as to where we'd like to go with MLS versus what we believe is feasible within the next 12-18 months
- Development and use of a working model!
 - A working model will provide a starting point

- MLS policies, procedures and processes so far are not adapted to the Network Enabled Operations philosophy that is being pushed forward. At the last NEOps Conference in December 2004, it was determined that people more than anything else were the bottleneck. It is the same for MLS. MLS proofs-of-concept must be developed in spite of current policies.

What is the most promising technology to begin implementing a solution in the short term?

- PKI
 - Not really
- Virtual Machines
 - Must find some way to (securely) share data between virtual machines
 - Even if the first model does not work it will be our starting point
 - Assuming that the transfer can only be carried out via manual cut and paste, the controls fall the realm of personnel and procedural security
 - Assuming that it can be done with COTS equipment
- PMI
 - Unfortunately most PMI is too rudimentary for useful MLS -- or any other - use.
- VM-based technologies
- Virtualization and data diode
- Guards and filters
 - Application level
- Without first an understanding of what may be accreditable, the question is hard to answer
 - We shouldn't limit ourselves by what is valuable now. VM technology wasn't in the 70s but was in the 90s. We need to move forward with solutions and get the criteria to evolve, as they must
 - If we get an idea of what may or may not be accreditable in various situations, then some areas can be progressed further while others can be dropped
- Web Servers for cross-domain information sharing
 - Proxies show a lot of promise in a lot of areas and should be pursued for web services as well as historic services (file, data, etc.)
- CFCS I project is already implementing a data diode (VETO) in their cycle 5 implementation. There is one installed so far, moving data across from DWAN to the TITAN network. For the operators needs, this solution is answering an urgent requirement to have access on the SECRET network to weather information and Geomatic data.
- Information encapsulation to provide partial data tagging to allow for semi-intelligent searching/sorting/storage

What would be the most promising MLS research areas of value to DND?

- The High-to-Low data transfer
 - Information flow would be the research area to examine/explore
 - Need to consider environment, procedures, and technology

- There is a WG that just stood up on IER starting at the operational level, but will look at all aspects of it. From that we could extract some information exchange requirements from the different security levels. Maj Jourdeuil from DGIMSP and Danielle Lemay from DEA are the lead
- Trusted computer base
 - Ditto
- Is Data Aggregation of interest?
 - A defined rule set to determine aggregates is very much of interest

What are the most important issues to be addressed at the next meeting?

- Progress made
 - If a larger government working group is established, any progress made or foreseen within other groups
 - And an established reporting mechanism
- Current state of the art on where MLS stands, assuming it's moved forward in six months to a year
- Brief what has been achieved in the proceeding time
 - See our MLS report [3]
 - The navy put one out as well
- New technologies available and the state of where our allies are
- The new technologies and progress towards MLS
- Certification opinions on various multi caveat/level security approaches
 - Unclassified level certification (e.g., Common Criteria), as well as input on High Assurance evaluation approaches (required for a classified solution)
- I've seen pieces to the puzzle, how do we put the pieces together to paint the picture
 - Perhaps a discussion that looks at the pieces and sees where things fit in a larger scheme, thereby determining what is/isn't available and where focused research should be applied
 - These pieces should be documented in a technical architecture so that they can be reused.
- Issues that are concrete and can be applied to a real solution(s), rather than just discussing the problems
 - Focused research and proof-of-concepts need to be funded in order to move things forward
 - Work share on funding and investigating various parts of the problem
 - I agree 100%. If you have a good case in mind, could you please share it with us? Obviously we cannot solve the entire MLS problem but there are solutions out there for specific requirements (e.g. http server) that can be easily accredited today
- Problems encountered with development
 - This should be defined by user community
- Developing business requirements
 - These are probably already defined, but need to be collected/collated and provided as a general guideline to future work
 - Has anybody done any work in this area and if they have documents they should be shared

- There was a great deal of work done in the 70s and 80s, and some into the 90s. It needs to be dredged up. DRDC Ottawa and CSSC (CSE) both did extensive work, as did NIST and NSA.
- Have there been accepted architectures for MLS that have evolved from current research?
- Research into real world MLS OSs and solutions being developed by companies today. It is doubtful whether the GoC can build its own solution without industry input.
- Next meeting should be closer to today, and have them more frequently; some more specific issues could be worked on and brought forward. It would also good if people from MLS research join in some other forums such as the CF C2IS integration Tiger Team to give updates to help orient the operational community on the way forward. This, in turn, would help DRDC to give direction to its research
- Industry initiatives - could have vendors brief where they are in this space
 - Industry solutions
 - An industry day could be hosted on the subject. With syndicate discussion between DND and industry on specific issues
- What would be needed is a way to synergize the work done by stakeholders. It is something that should be determined at this meeting, not the following
 - A quick follow-on meeting, within 3 weeks, would resolve this and help move things forward and create momentum, that's needed.
- A database on works done with respect to MLS or information domain separation within DND and OGDs
 - Or at least a single web page to visit with all the necessary links.

What are the characteristics of the Certification& Accreditation process?

- You don't want to know
- This is the most important question
- No comment
- It's a secret
- Minimize risk to an acceptable level for control/management, then get someone to sign off as accepting the responsibility
- If we fully understand we will be able to determine a better way ahead
- Talk to your C&A people early and often, keep them in the loop on any initiative so that they have a harder time telling you "No" at the end
 - Were not all that bad
- The criteria were designed to be flexible. As such, the criteria need to be pushed as opposed to the evaluators pushing what is acceptable. The criteria should not be viewed as strictly defining what is possible but rather the functionality of what can be evaluated. If it is not possible, according to C&A authorities, they're wrong. Trust me
- Implicit threats defined through security policies
- Lack of senior management sign-off on high risk alternatives
- At CSE, there is an evaluation program (CCEP) for High Assurance products. Once a product is evaluated, the report is forwarded to the C&A folks, who most often will act upon the recommendations of the evaluators. However, the CCEP is geared

towards Type 1 products, and it is uncertain whether this "MLS solution" will fall into that category, as it may not be a crypto product

- Operational authorities retain the option of circumventing the C & A process by agreeing to accept full, sole responsibility for any problems operating the system.

What would be the characteristics of a better C&A process? How can this be implemented?

- Efficient, fast, cogent C&A that is consistent between departments, organizations, etc. Perhaps too much to ask?
 - Assuming any solution will be the same across departments
 - Much like TRAs, two individuals usually produce two different results. It's not a science but more an art
 - While not increasing risk
 - Not if they are properly following the CAG. This eliminates the grey matter
 - Then it should be automatable
 - It has! It has almost been reduced to a check list
 - Check lists are used to confirm that content of the required documents have addressed the security/risk reduction criteria. Answers recorded in checklists are generally used as input to the threat-risk assessment portion of the process, the output of which is the 'residual risk' that then is the determining factor if the 'system' is certifiable and accreditable
 - This is not something that can be rushed. System familiarization takes time
 - Define success criteria and get the C&A people to sign off
 - Understanding by EVERYONE that there is "good enough" and that it's acceptable
 - Implies someone is willing to accept responsibility/accountability for 'good-enough'
 - And define "good enough" to the stakeholders.
 - DO your security engineering properly.
 - In consultation/collaboration/partnership with certification authorities and accreditation authorities - recall it is a two-part process.
 - Get C&A people involved early, but also make sure they can understand the technicalities of the solution
 - C&A is the independent review that due care has been exercised to meet the baseline security requirements. Under the GSP, deputy heads are responsible for security in their dept. The Dept Security Officer, and the IT Security Coordinator, manage the dept security program on behalf of the deputy head(s). Better high level visibility of compliance within the dept is necessary, and was raised as one of the major observations in the last OAG report.
 - If the objective is to bypass good security practices, then it needs to be brought to the DM/CDS's attention, and reported to TB on a periodic basis. DND, along with

most other depts, has already been observed upon for failing to provide this kind of feedback

- If the core security and functional requirements have been properly defined, and the developed solution maps to the requirements properly, C&A should not be a hindrance. All C&A requirements should be designed into the system.

Appendix D: Meeting Agenda

Agenda for the
Second DRDC Meeting on Multi-Level Security (MLS)
April 6, 2005
Defence R&D Canada
DRDC Ottawa
Shirley's Bay Campus
3701, Carling Avenue
Ottawa

Directions may be found at: http://www.ottawa.drdc-rddc.gc.ca/about/traveling_e.asp

- | | |
|---------------|--|
| 9:00 – 9:30 | Check in and coffee (Building 5, conference room A). Please be at the Guardhouse no later than 9:10 A.M.) |
| 9:30 – 9:45 | Welcome, Administrative Information, and Meeting Organization/Objectives, Karim Dahel, NIO Section, DRDC Ottawa |
| 9:45 – 10:20 | MLM: Coordinating Network Management across Security Boundaries using Policy Resolution, David Kidston, CRC |
| 10:20 – 10:40 | Coffee break |
| 10:40 – 11:00 | Segregation & Hardening of Systems via Virtual Machines, Eugene Bacic, Cinnabar Networks Inc. |
| 11:00 – 11:35 | Overview of some MLS architectures and MLS solutions, Jean Savoie, NIO Section, DRDC Ottawa |
| 11:35 – 11:55 | A trusted user monitoring system with biometrics, Qinghan Xiao, NIO Section, DRDC Ottawa |
| 12:00 – 13:00 | Lunch Break
<i>Lunch (no-host) is available onsite at the CRC Cafeteria</i> |
| 13:00 – 14:30 | Focused discussion on some MLS issues and solutions |
| 14:30 – 14:50 | Coffee break |
| 14:50 – 15:20 | Wrap-Up |

UNCLASSIFIED

SECURITY CLASSIFICATION OF FORM
(highest classification of Title, Abstract, Keywords)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.) Defence R&D Canada – Ottawa Ottawa ON K0A 0Z4		2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable) UNCLASSIFIED
3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.) Defence R&D Canada Second-Multi-Level Security Meeting, April 6 2005 (U)		
4. AUTHORS (Last name, first name, middle initial) Savoie, Jean		
5. DATE OF PUBLICATION (month and year of publication of document) December 2005	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.) 90	6b. NO. OF REFS (total cited in document) 4
7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) DRDC Technical Memorandum		
8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.) DRDC Ottawa, Network Information Operations Section, 3701 Carling Avenue Ottawa K1A 0Z4		
9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant) 15bq02 and 15bq03	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)	
10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC Ottawa TM 2005-249	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)	
11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification) ☒ (X) Unlimited distribution ☐ () Distribution limited to defence departments and defence contractors; further distribution only as approved ☐ () Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved ☐ () Distribution limited to government departments and agencies; further distribution only as approved ☐ () Distribution limited to defence departments; further distribution only as approved ☐ () Other (please specify):		
12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.) Unlimited		

UNCLASSIFIED

SECURITY CLASSIFICATION OF FORM

DCD03 2/06/87

UNCLASSIFIED

SECURITY CLASSIFICATION OF FORM

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

The Second Multi-Level Security (MLS) meeting in a series was held on April 6, 2005 at Defence R&D Canada (DRDC) Ottawa. The purpose of these meetings is to bring together researchers, developers, and practitioners in multi-level security (MLS), from both military and civilians sectors, and to provide a forum for dialog and interchange. The second meeting theme was short-to-medium term solutions for current MLS issues for the Department of National Defence or organizations within the Canadian government. The second meeting's invited presentations, discussions and questions to participants are provided and analysed. Moreover, a conclusion and a motivated recommendation are given. It is recommended that a multi-security domain working group be established.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

MLS, Multi Security domains

UNCLASSIFIED

SECURITY CLASSIFICATION OF FORM

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale



www.drdc-rddc.gc.ca

